AVAYA
Communications Server 1000
Release 7.5

Installation, Configuration,
Support & Troubleshooting

Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

1

Copyright Amlex Associates Ltd

Notice of Rights

All rights reserved. No part of this manual, including interior design, may be reproduced or translated into any language in any form, or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without prior written permission of Amlex Associates Ltd.

This manual is subject to the condition that it shall not, by way of trade or otherwise, be lent, sold, hired out or otherwise circulated without the prior consent of Amlex Associates Ltd, incomplete nor in any form of binding or cover other than in which it is published and without a similar condition including this condition being imposed on the subsequent receiver.

All brand names and product names used in this book are trade names, service marks, trademarks or registered trademarks of their respective owners.

Contents

1-1. Introduction & Architecture	3	2-16. UCM Users & Roles	177
1-2. System Components	19	2-17. UCM Deployment Backup	183
1-3. Building an SA or HA System	39	2-18. Linux CLI	187
1-4. Command Line Interface	47	2-19. Patching	192
1-5. Initial Call Server Config	56	2-20. CoRes Call Server	203
1-6. Linux Base Installation	67	2-21. Virtual Trunks	219
1-7. Security Configuration	85	2-22. Network Routing Service	243
1-8. Software Deployment	104	3-23. Avaya Aura Migration	260
1-9. Adding Media Gateway	113	3-24. PRI Trunks	287
2-10. Joining the UCM Security Domain	130	3-25. NFS Deployment	296
2-11. IP Telephony Node	133	3-26. Media Application Server	302
2-12. Configuring Sets	145	3-27. Maintenance & Diagnostics	333
2-13. List Manager	155	3-28. SIP Line Gateway	347
2-14. Subscriber Manager	158	3-29. System Redundancy	358
2-15. Corporate Directory	172	3-30. PCAP - Packet Capture	373
		Appendix	380

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

2

Notes

_____

_____

_____

_____

1. Introduction & Architecture

- Communication Server Documentation
  - Using NTP's
- Overview of Meridian & CS1000 systems
  - Large & Small switches
  - CS1000
- Internal Addressing
  - Terminal Numbers
  - Loops & Superloops
- Call Flows
  - Telephony Node – Terminal Proxy Server
  - Network Routing Service
- Unified Communications Manager (UCM)
  - Security Domain
- System & Session Manager
  - Alternate Primary Security Server / Deployment Server
  - Alternate Network Routing Service
- IP Telephony Node

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

3

Notes

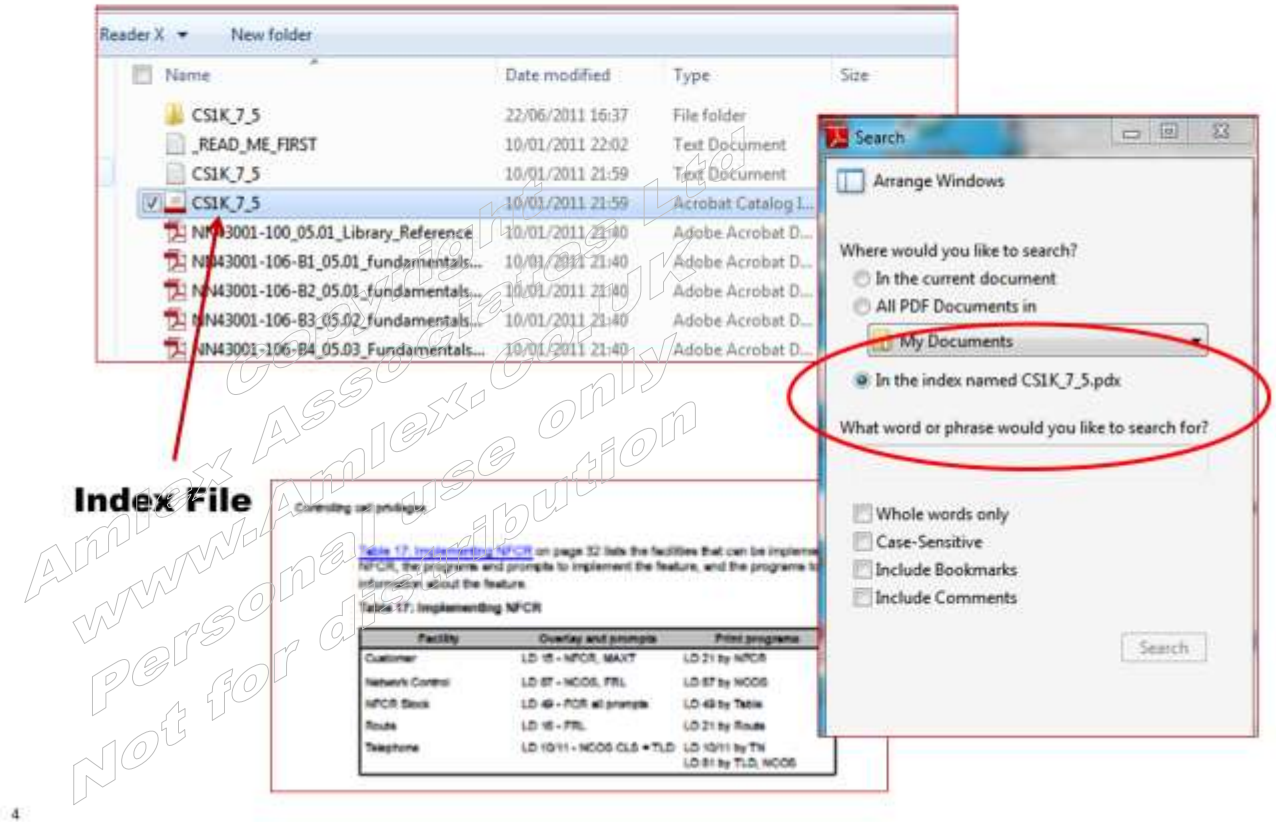
Documentation – NTP's

Avaya produce a very comprehensive range of documentation for all of their systems.

Previously they supplied an application known as Helmsman which was used to search the archive of documentation for the relevant information.

However since Release 5, the Helmsman application has been discontinued and Technical Publications are delivered with an Adobe Acrobat Index file which is used as the search tool.

By opening the .PDX Index file you will be offered the search dialogue seen above. By selecting the option to search in the Index file, all documents will be referenced and all occurrences returned.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

CS1000

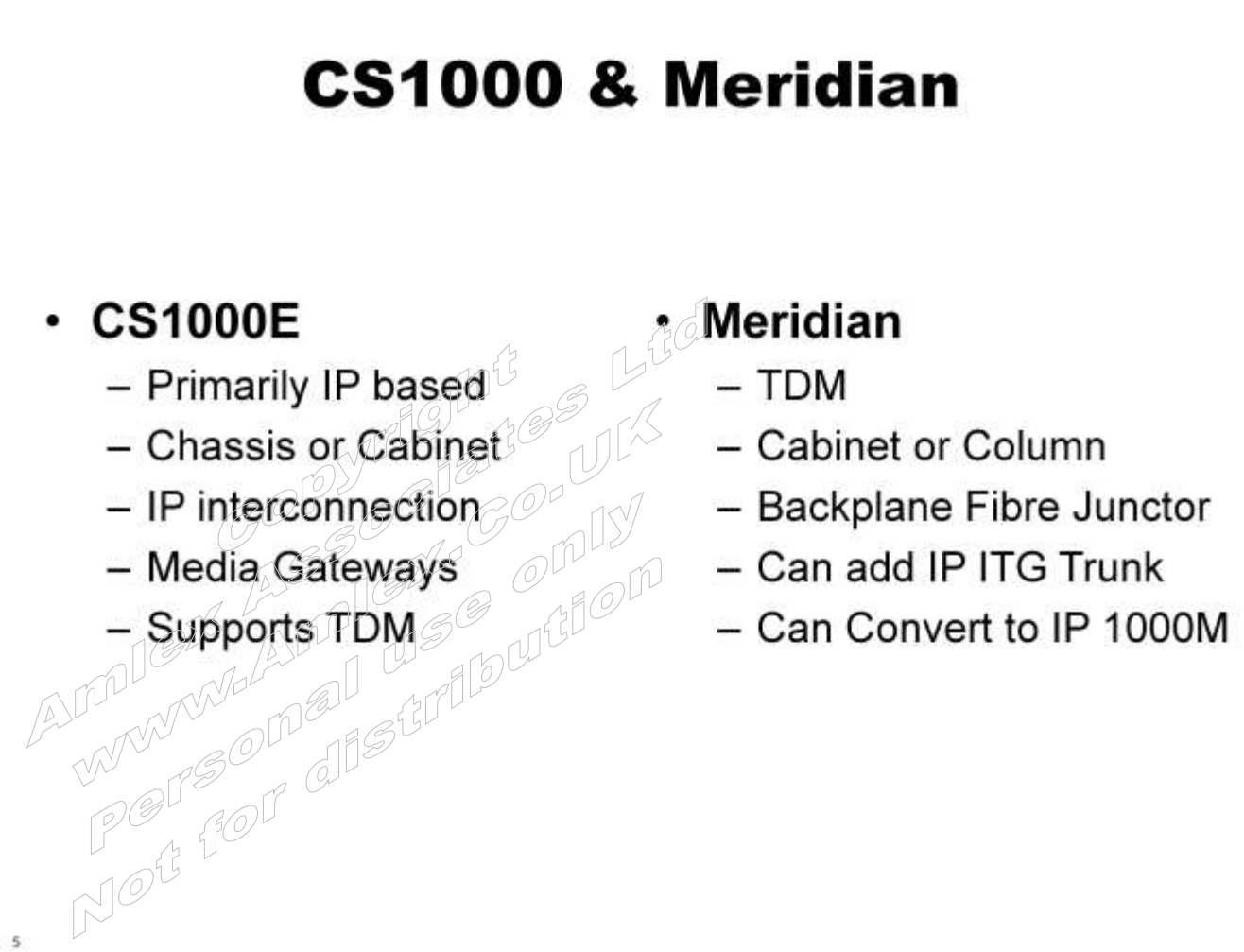
The Call Server 1000 is Nortel's Heritage IP based PBX and can be configured for up to 40,000 users. It is a distributed architecture using standard IP for all primary interconnections.

Meridian 1

The Meridian PBX is primarily a TDM device with the option of adding IP trunks or converting to full VoIP operation.

Both devices share a lot of components such as Cabinets and Chassis, Intelligent Peripheral Interface (IPE) cards, CPU's and terminals.

The core of the operating system is essentially the same across both platforms with a few differences to accomodate for the differing hardware.



Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Architecture Overview Meridian

The Meridian comes in two distinct types, the Large Switch Dual Processor (Option 8100 & 6100) and the Small Switch Single Processor (Option 11).

The primary differences are the actual CPU board and physical layout.

Option 11 Small Switch

Uses a Small System Controller and is housed in the Cabinet or Chassis. It can comprise of multiple cabinets or chassis which are inter connected.

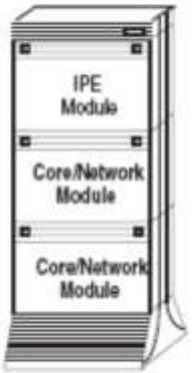
A Small switch only uses Card and Unit numbers to define a TN and these are linked to the cabinet slot.

Option 8100 & 6100 Large Switch

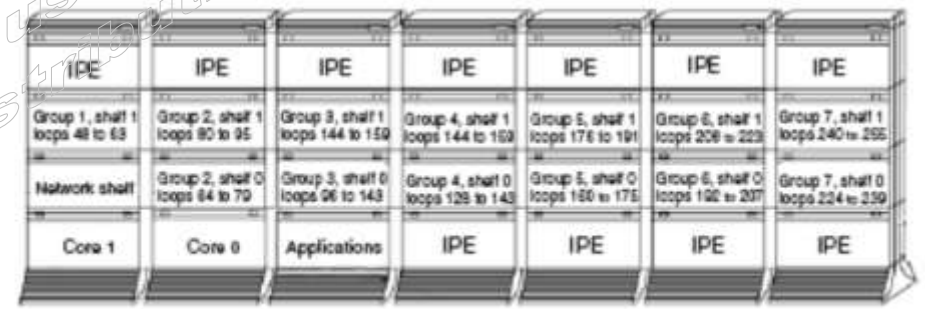
At release 5 only the Pentium ii & iv may be used as the CPU. As large switches they use Loop Shelf Card and Unit to define each TN. The system is consists of Columns of Shelves.

On a large multi group system Shelves are interconnected using Fibre Loop (previously Junctor Board).

Small Systems



Large Systems


IPE
IPE
IPE
IPE
IPE
IPE
IPE
Group 1, shelf 1 loops 48 to 63
Group 2, shelf 1 loops 80 to 95
Group 3, shelf 1 loops 144 to 159
Group 4, shelf 1 loops 144 to 159
Group 5, shelf 1 loops 176 to 191
Group 6, shelf 1 loops 208 to 223
Group 7, shelf 1 loops 240 to 255
Network shelf
Group 2, shelf 0 loops 64 to 79
Group 3, shelf 0 loops 96 to 143
Group 4, shelf 0 loops 128 to 143
Group 5, shelf 0 loops 160 to 175
Group 6, shelf 0 loops 192 to 207
Group 7, shelf 0 loops 224 to 239
Core 1
Core 0
Applications
IPE
IPE
IPE
IPE

Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

6

Notes

_____

_____

_____

_____

Architecture Overview CS1K

The CS1000 is always a “Large Switch”, in other words it always expects TN’s (Terminal Number – internal address) to be in the form of Loop, Shelf, Card, Unit.

The internal connections of the system (ELAN – Embedded LAN) between different components such as the Call Server, Media Gateways and Signalling Servers is established using IP and Ethernet only. In this way a CS1000 can be deployed in a distributed fashion across a network.

Media Gateway – Houses the Cards for the system, essentially the TDM resources. Controlled by the Media Gateway Controller. It also contains the **Media Cards/DSP boards** which allow the conversion between the two environments. A media Card channel is required for every IP to TDM call in progress.

Signalling Server – acts as the intermediary between the Call server and the IP sets. In addition it provides the signalling required to set up Virtual Trunk Calls.

- Large Switch
- InterSwitch Links IP
  - MG CS SS etc
- Distributed Architecture
- Cabinet Or Chassis
- Media Gateway
  - Houses TDM devices
  - Media Card TDM ⇔IP
- Signalling Server
  - Intermediary between Call Server & IP Phones and Virtual Trunks

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

7

Notes

_____

_____

_____

_____

Terminal Number - TN

The internal addressing of the system is done using Terminal Numbers.
Actual TN's are defined by the number of Loops a system has and its configuration.

On all release 5 and later CS1000E systems this will be 256 loops (0-255), however on Meridian systems this may be smaller.

TN's are used to address cards & units on the cards. A normal TN can be traced to a physical port on the system itself.

Virtual TN's on the other hand are used to address devices where there is no discrete physical connection port such as IP telephones and Virtual Trunks.

This does mean that some correlation needs to be made between the Virtual TN of an IP Set and its IP address. This is done by the Terminal Proxy Server (TPS discussed later) on the Signalling server at set registration time.

- A TN on a Large Switch comprises of :
  - LOOP SHELF CARD UNIT
    - E.G. 8 0 4 0
- A Small Switch only uses
  - CARD and UNIT designation
    - E.G. 5 1
- Virtual TN's are used for IP Sets & Virtual Trunks as there is no physical port
  - A Virtual Superloop can have the maximum number of TN's available

LOOP	SHELF	CARD	UNIT
1	1-0	0-15	0-31

  - Total TN's/Superloop = 1 x 2 x 16 x 32 = 1024

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

8

Notes

Copyright Amlex Associates Ltd

Loops

The system has 256 loops which are used to define the individual addresses of devices. Loops are still used for certain devices to address them rather than a TN notably PRI loops and Tone & Conference Loops.

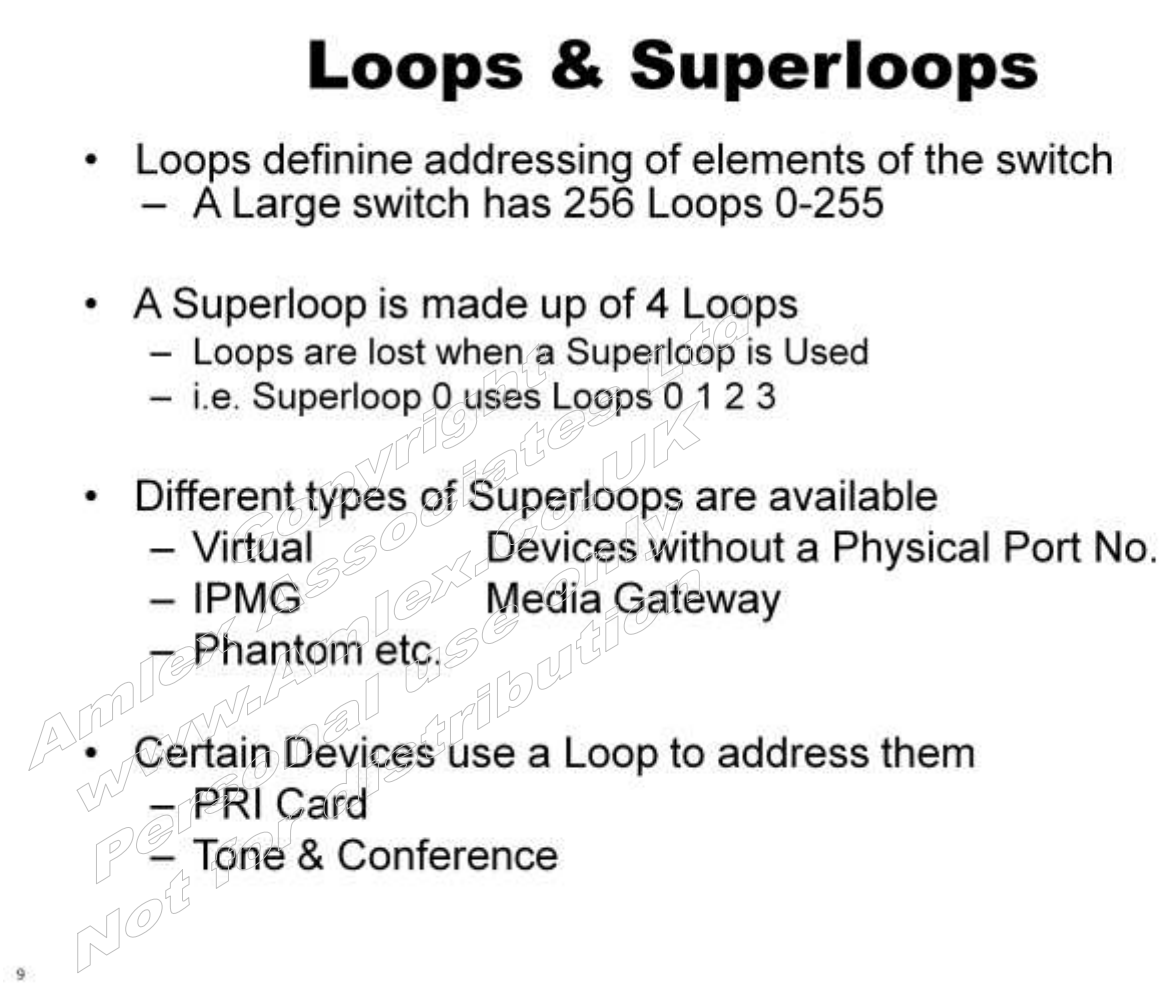
Superloops

As the original system grew the concept of a Superloop emerged which was created by combining 4 Loops. Once combined the contributing Loops would be unavailable.

We can use different types of Superloop but two which are essential for the CS1000 are the IPMG Superloop and the Virtual Superloop.

IPMG Superloop – Links the IP address of the Media Gateway Controller to a Superloop. Each Media Gateway consumes half a Superloop i.e. Shelf 0 or 1.

Virtual Superloop – Is used for devices which have no specific physical port such as IP sets and Virtual Trunks.


Loops & Superloops
• Loops definine addressing of elements of the switch
– A Large switch has 256 Loops 0-255
• A Superloop is made up of 4 Loops
– Loops are lost when a Superloop is Used
– i.e. Superloop 0 uses Loops 0 1 2 3
• Different types of Superloops are available
– Virtual Devices without a Physical Port No.
– IPMG Media Gateway
– Phantom etc.
• Certain Devices use a Loop to address them
– PRI Card
– Tone & Conference
9

Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

The ELAN (Embedded LAN) is a private management network whilst the TLAN (Telephony LAN) is connected to the "Public" side. Telephones maybe connected to the TLAN directly or to a network routed from the TLAN (Sometimes referred to as the CLAN Customer LAN).

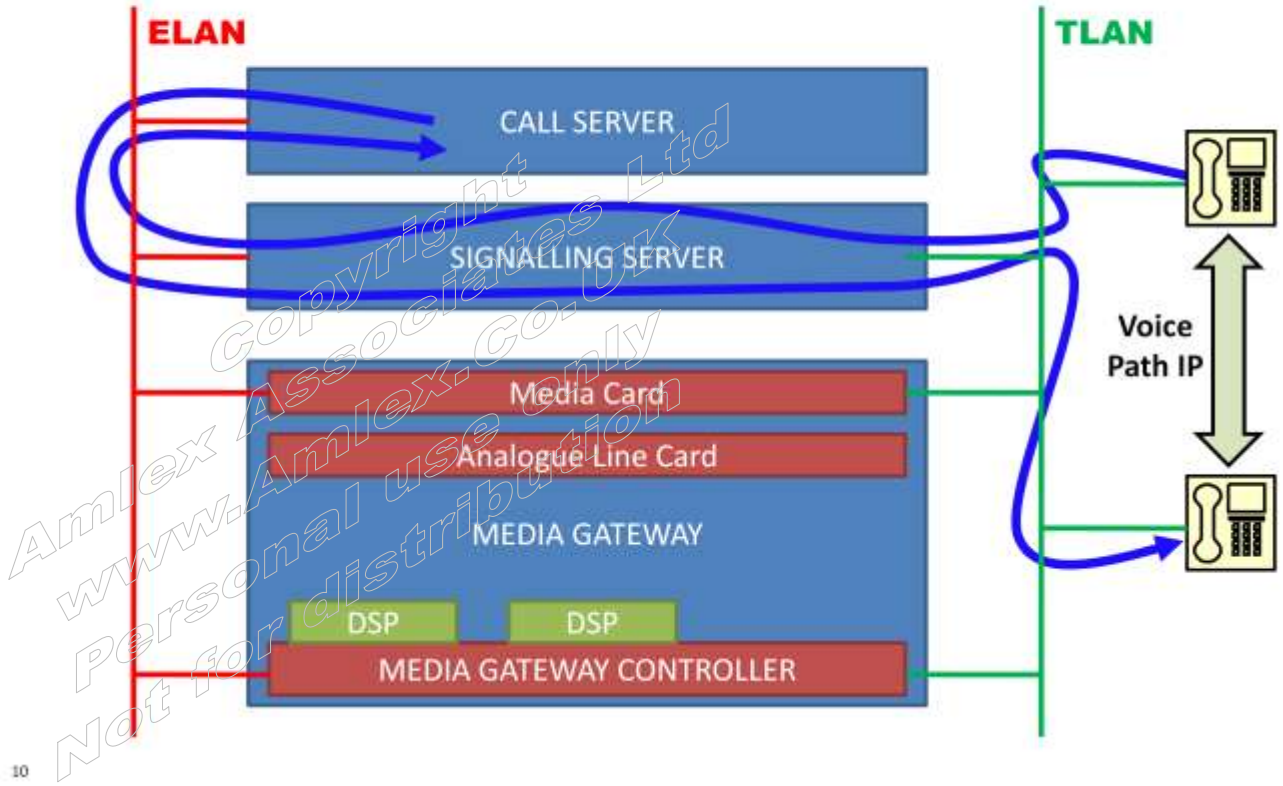
IP Sets need to communicate with the Call Server to make and receive calls and this is done by registering with the Signalling server.

The Signalling server runs several pieces of software but the sets use the TPS, Terminal Proxy Server to register with and to communicate with the call server. The TPS records the IP address of the Set and its Virtual TN so the Call Server can contact it via the VTN.

For an IP to IP call the set will contact the Call Server via the TPS. The Call server will look up the VTN of the destination set and refer it back to the TPS which will contact the set.

When the call is established the voice travels directly from IP Set to IP Set and NOT via the sig server or call server.

IP to IP Call



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

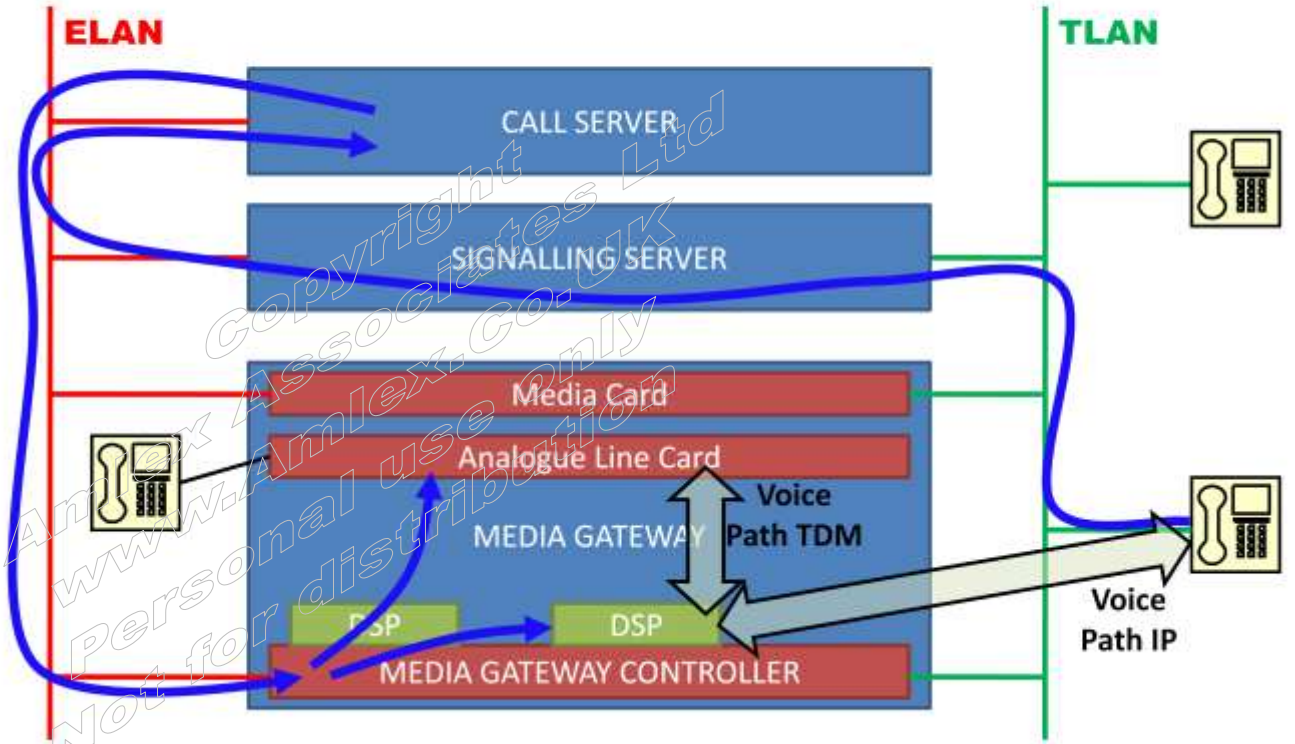
_____

_____

_____

IP to TDM Call

If the end point is a TDM set the call server messages the Media Gateway to allocate TDM/IP resource as well as signalling the traditional set. The Voice path for the completed call would be via a Media Card as shown.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

11

IP ⇔ IP
IP Set to TPS with Dialled no.
TPS passes to Call Server
Call Server looks up Dialled No.
Call Server returns VTN to TPS
TPS signals Destination IP set
Codecs agreed
Zone Bandwidth Allocated
Destination picks up
Voice path established directly IP-IP

IP ⇔ TDM
IP Set to TPS with Dialled no.
TPS passes to Call Server
Call Server looks up Dialled No.
Call Server contacts Media Gateway with TN of set
Media Gateway signals destination & allocates DSP (Media Card) resource
Codecs agreed
Zone Bandwidth Allocated
Destination picks up
Voice path established directly IP-DSP
DSP-TDM resource

Notes
_____
_____
_____
_____

Virtual Trunks are used to carry VoIP calls between systems without the need for conventional circuits just using IP networks.

This diagram shows the basic flow for a Virtual Trunk IP to IP call. Set 1000 is calling set 2000.

Set 1000 signals the call server via TPS on the Sig Server

Call server identifies 2000 as a remote set and sends the call to the Virtual trunk gateway (SIP or H.323) on Sig Server.

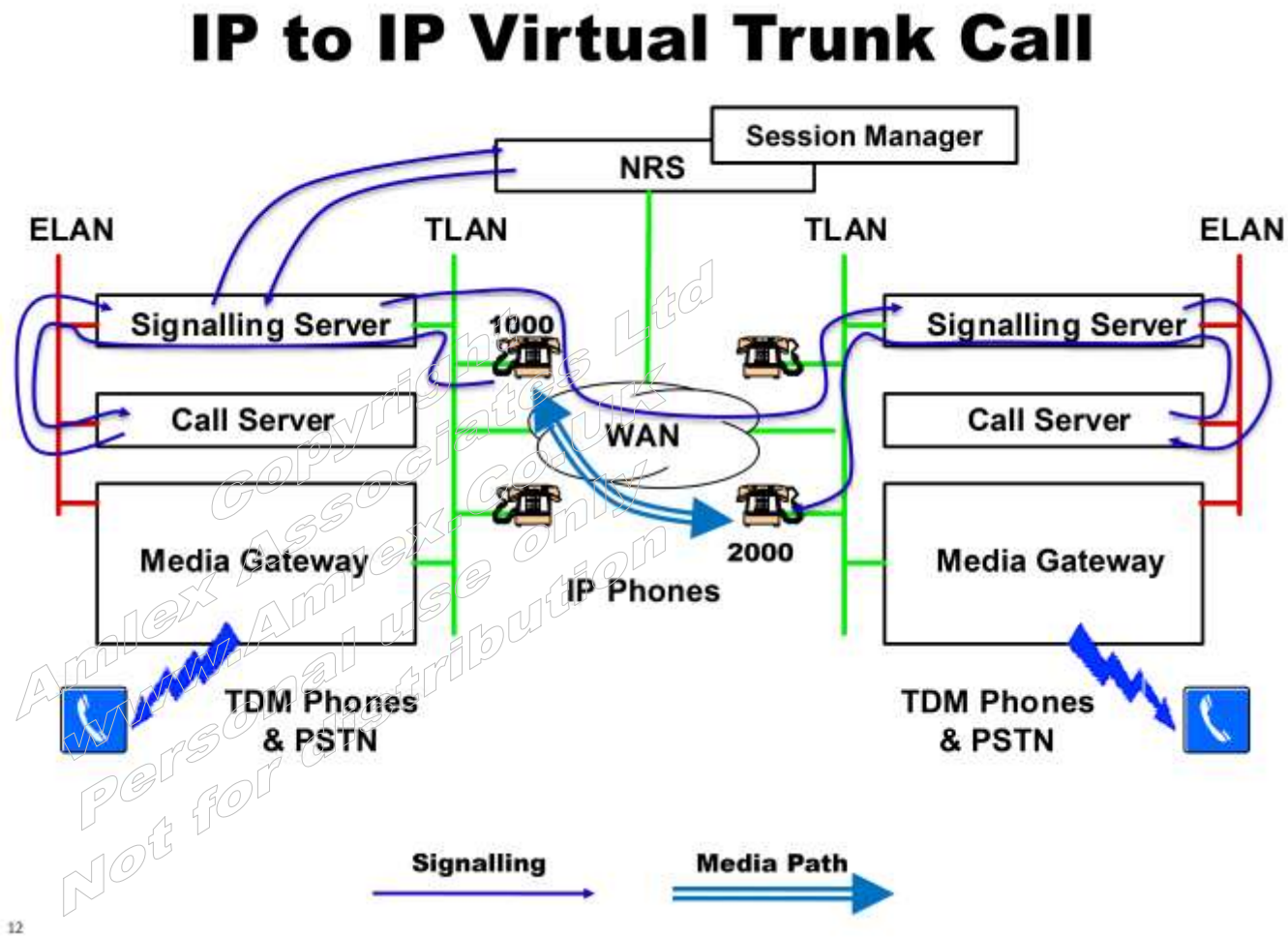
Sig server sends request to the NRS (Network Routing Service) to identify where 2000 is. (In Aura networks this would be the Session manager)

NRS responds with the IP address of the destination Signalling gateway.

The Signalling gateway on the initiating system then contacts the Signalling gateway on the destination system.

Request is sent to the CS on destination as an inbound D-Channel.

CS looks up set 2000 and then sends a call setup to it via the TPS on its Signalling server.



Amlex Associates Ltd Copyright
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Unified Communications Manager

The UCM framework adds a complete management and Security Domain to the CS1K environment defined by the Primary UCM which can be a CS1K Linux server or Aura System Manager.

It controls access to the systems and servers as well as regulating communications between them.

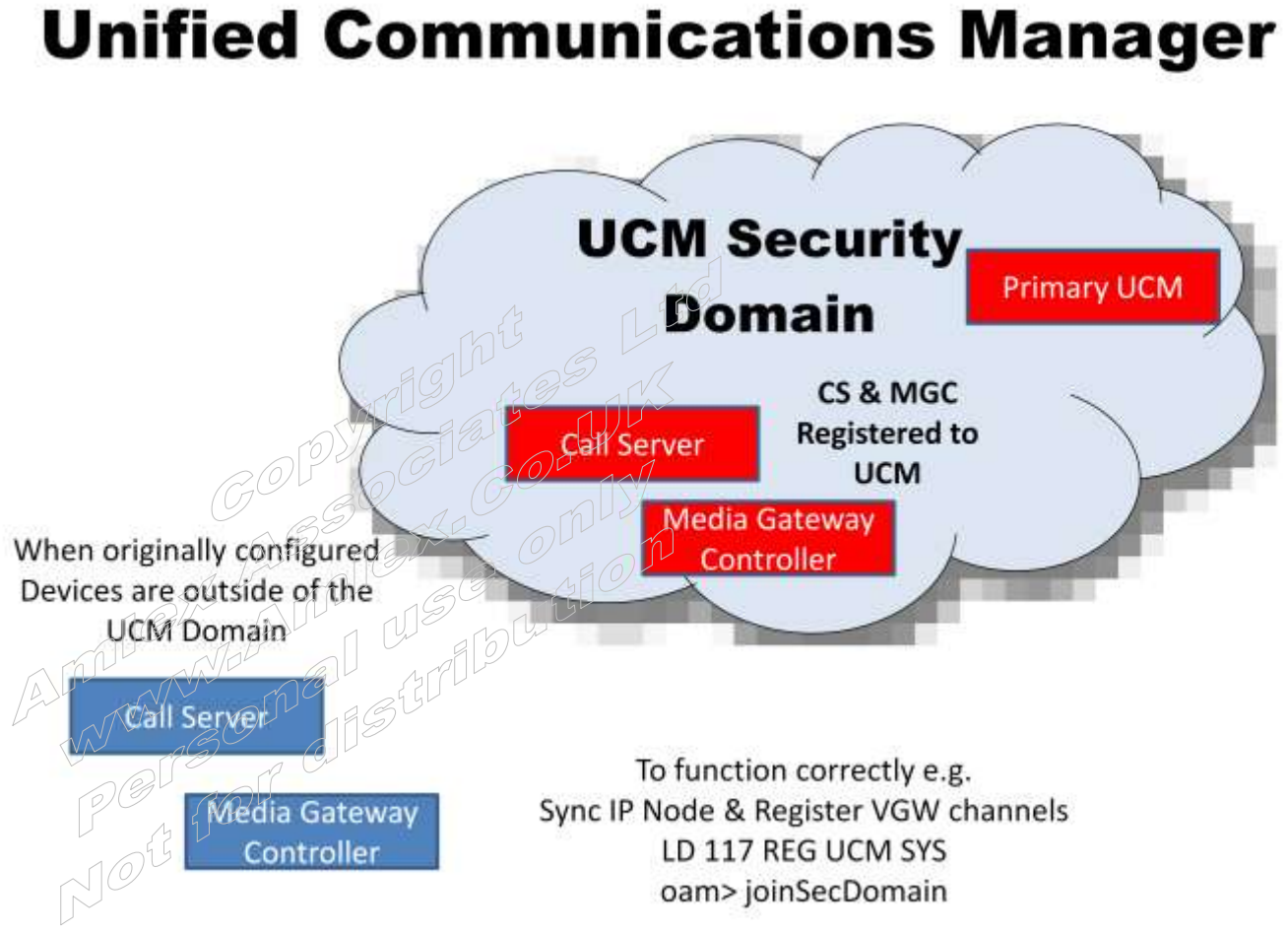
When the component devices are initially configured (Call Server, Media Gateway etc) they are outside of the UCM domain but can communicate at a basic level. For full functionality however they must be added to the UCM domain. This is done in one of two ways

LD 117 REG UCM SYS

Or on the command line of the device e.g. MGC card

oam> joinSecDomain

These commands complete the registration of the devices to allow SSH communications between them. Specifically IP Node synchronisation and MGC configuration download.



Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Once the UCM security Domain is established the Primary UCM server controls all communications and authorisation.

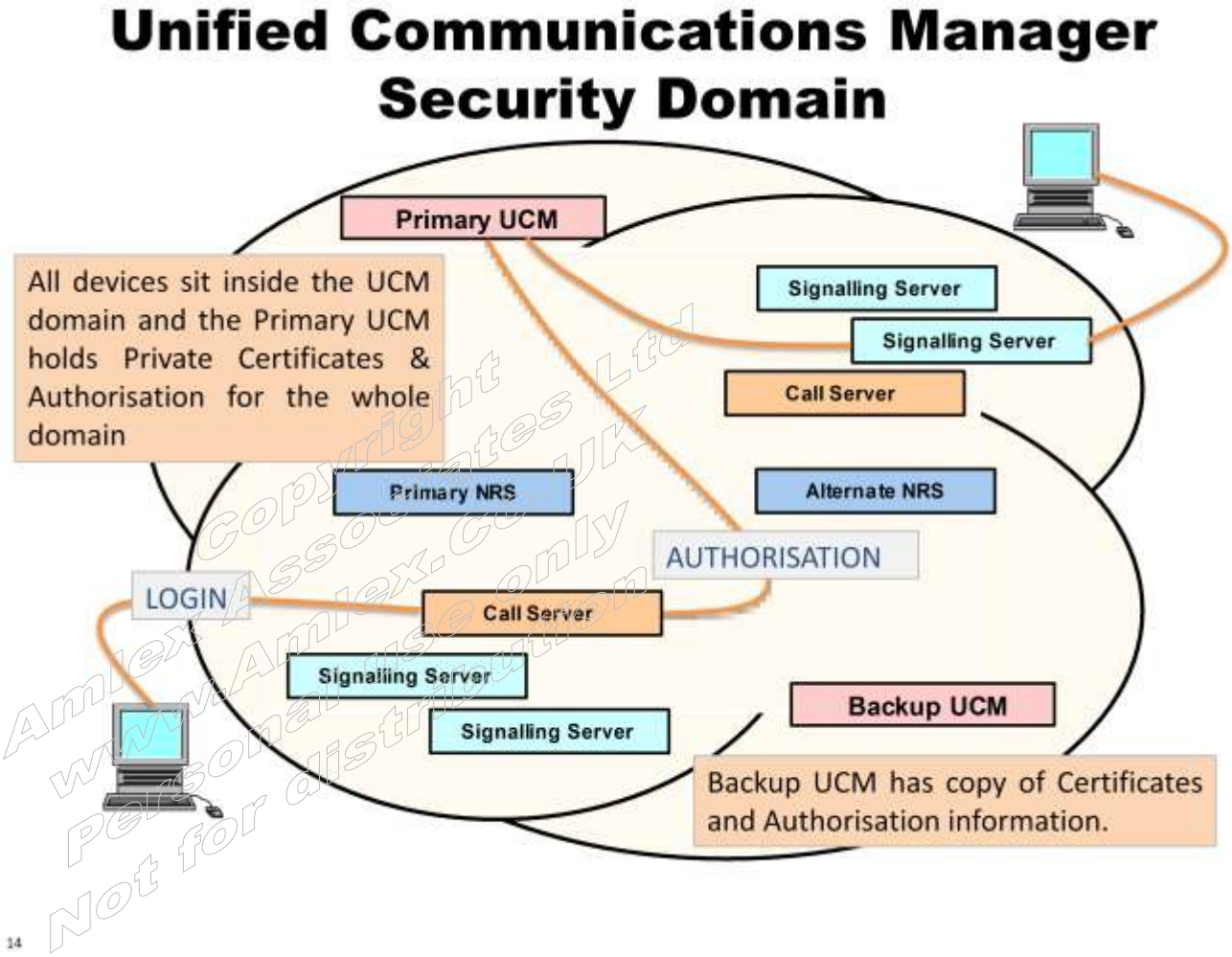
If a user tries to login to a signalling server or call server as shown in the diagram, their login credentials will be passed to the Primary UCM for validation and Authorisation.

In this way a call server created with a new default database will have the users “admin2” & “admin1” available.

However once the Call server has been registered within the security domain it will only have the user “admin” available for login until further UCM users are created.

In essence the Primary UCM runs a RADIUS server which is used for the Authorisations. In the event that a failure occurs and the Primary UCM cannot be reached in a CS1K implementation the Backup server will be contacted for authorisation as it has a copy of the database. If the Backup is unavailable then an “Emergency” account is used to login to the server.

The Aura System manager has its own redundancy scheme.



Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

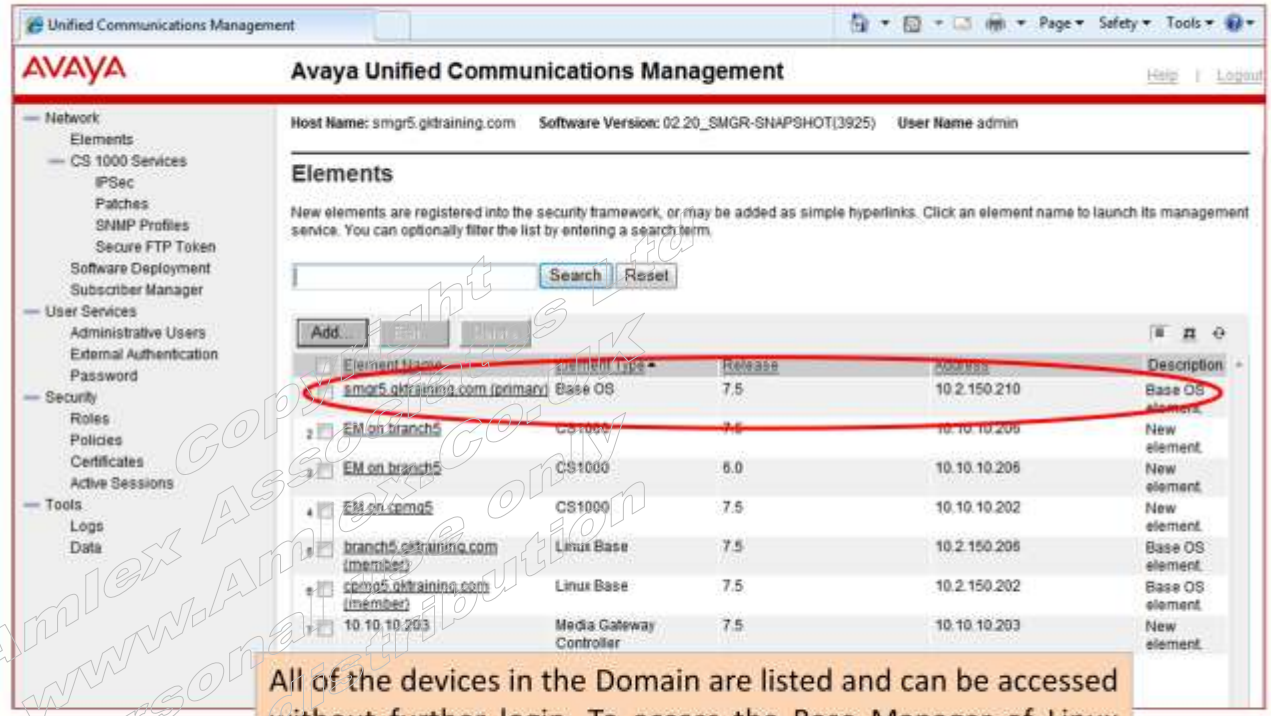
Element List

Devices that have become part of the UCM domain are added automatically to the Elements list shown here.

This can be used to access the different servers and the services running on them such as the Base Linux, NRS or the Element Manager

Note the Media Gateway has been added to the Elements list but is not a link (i.e. Not underlined). Thus it cannot be clicked on to gain access to the device. This is the same with VxWorks based Call Servers.

No further login is required to access the elements, this is known as Single Sign On or SSO.



All of the devices in the Domain are listed and can be accessed without further login. To access the Base Manager of Linux Elements click on the Links to Element Types Linux Base.
NOTE:- The screen shown is from an Aura installation hence the System Manager Element (SMGR5 - Base OS)

15

Notes

_____

_____

_____

_____

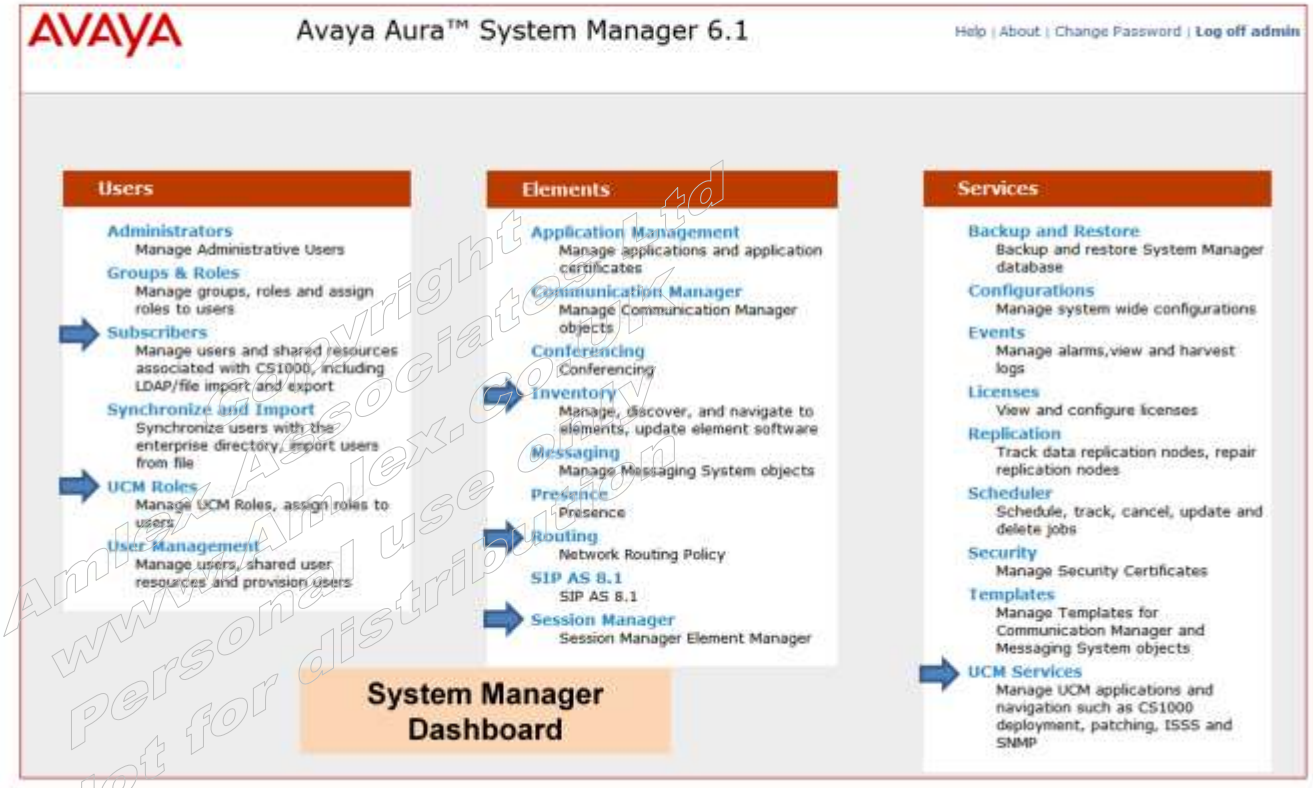
Copyright Amlex Associates Ltd

System Manager

System Manager is the management interface for the Avaya Aura system integration suite of communications programmes .

When CS1K is implemented through Aura this will be the Primary UCM element and the login screen for management. Thus it will deal with the Authentication, Authorisation and Accounting for the system as well as the Certificates for the different Elements.

The Highlighted menu options are the primary elements used for managing a CS1K implementation via System Manager.



Amlex Copyright Amlex Associates Ltd www.amlex.com Personal use only Not for distribution

Notes

_____

_____

_____

_____

Session Manager

The Aura Session Manager is the SIP Proxy core of the Aura architecture and plays a key role in orchestrating communications between different elements of the system.

Its role is equivalent to that of the Network Routing Service (NRS) excepting that it does not deal with H.323 call routing. For the CS1K it effectively replaces the SIP Proxy or Redirect server and the Network Connect Server (NCS) elements of the NRS.

Session manager always works as a full SIP proxy and has mechanisms to monitor the connection to the SIP entities it is managing as can be seen here. This is the reverse of the situation for endpoints on the NRS which constantly Re-register ensuring the system knows they are still available for call processing.

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

17

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

The **Node ID** is a number of up to 4 digits used to identify the Telephony node. The **Node IP Address** is a TLAN address but not the TLAN address of the sig server itself and represents the whole node.

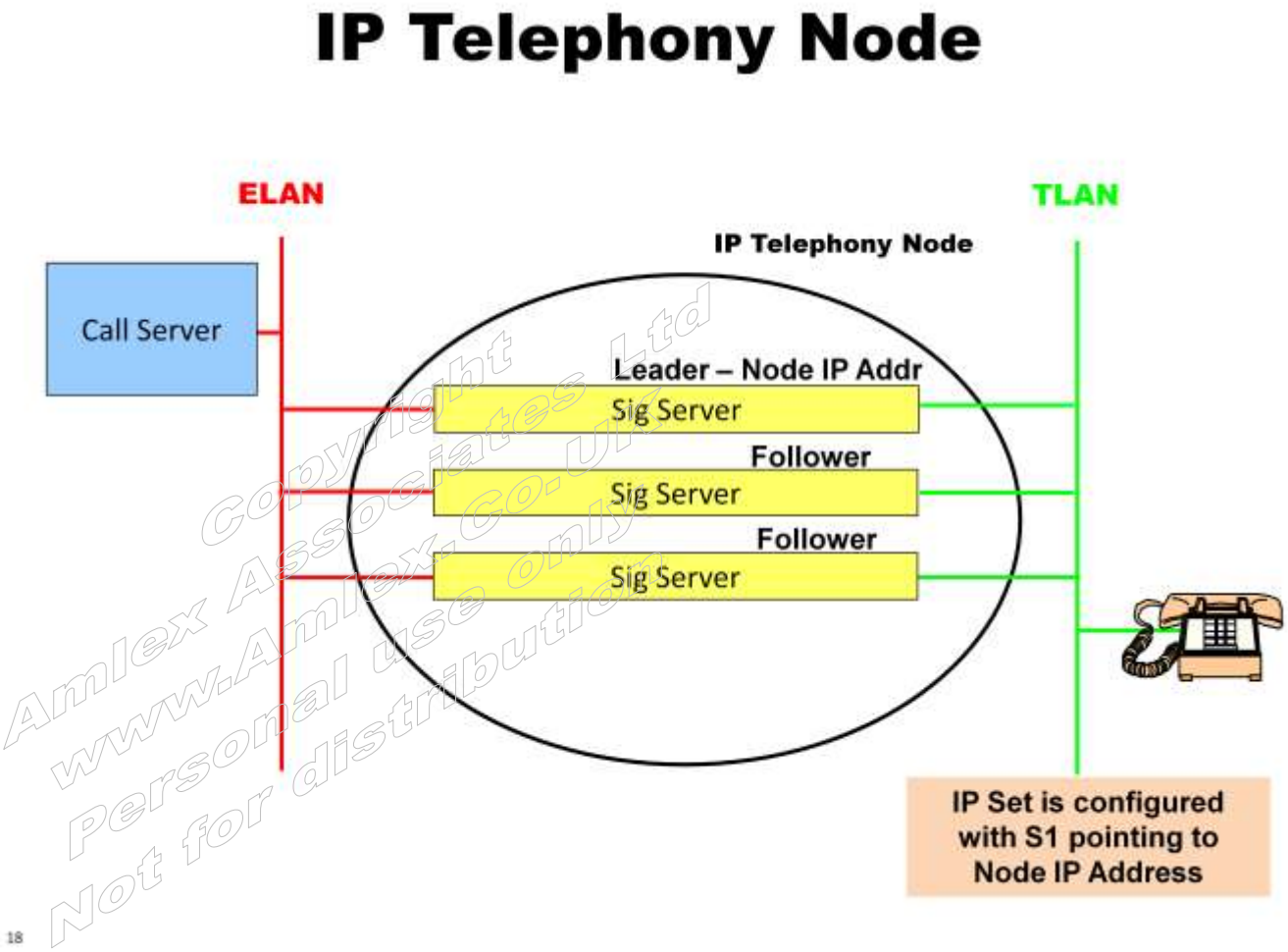
The **Node IP Address** is held by the **Leader** signalling server of the IP telephony node.

Devices in the Node are either a **Leader** (one only) or **Follower**. In the event of a failure of the Leader the Followers will elect a new Leader which will then assume the Node IP address as well as its own TLAN address.

The IP sets are configured to connect to the IP Node address for registration, thus even in the event of a Sig server failure the IP Node address will still be available via the new **Leader**.

All of the devices running TPS are included in the IP Telephony node.

A system can have multiple IP Nodes if required.



Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

2. System Components

- Call Server
  - Customer Database and ultimate Call Controller
- Linux Server
  - UCM & Common Services
  - Platform for various applications
    - Signalling Server
      - Line Terminal Proxy Server
      - Virtual Trunk Signalling Gateway
      - Personal Directory
    - CoRes Call Server
    - NRSM
    - SIP Line Gateway
    - IM & Presence
- Media Gateway
  - Houses IPE (Intelligent Peripheral Equipment) Cards
  - Houses Media Cards which convert from IP to TDM

19

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

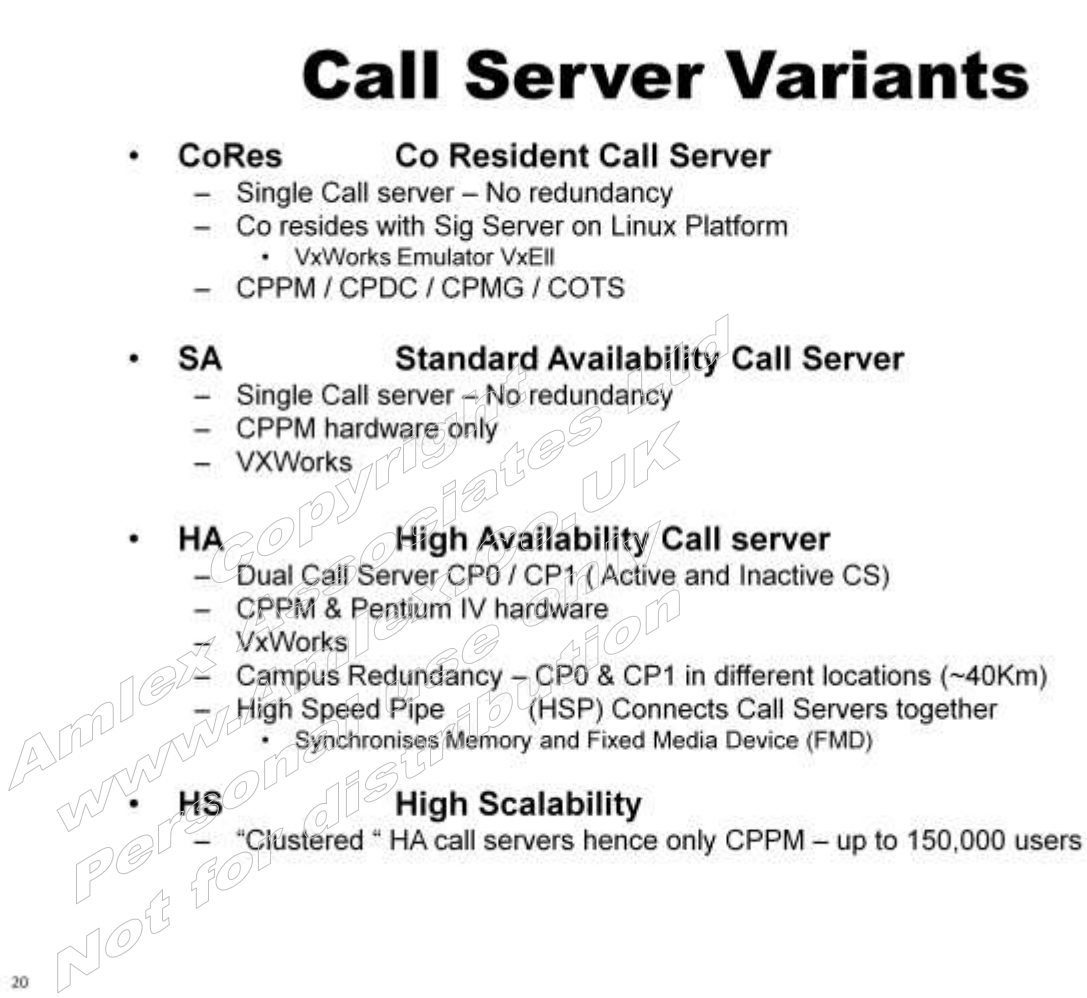
Release 6 introduced the CoRes Call server with both the Call server and Signalling server resident on the same CPPM card running Linux. This is achieved using a VxWorks emulator (VxEll). Release 7 enhances this with new hardware.

The Standard Availability call server can support up to 40,000 users and has a single CPPM card running VxWorks.

The High Availability call server adds a second redundant CPU to enable failover as well as well as reducing downtime for system upgrades.

HA is sometimes referred to as Campus Redundancy when the CPU's are housed in different locations. The maximum distance is defined by the speed of the High Speed Pipe link which ensures the memory and FMD (Fixed Media Device) are constantly synchronised.

HS is a Rel 7 feature allowing the "Clustering" of HA systems for even greater user numbers.


Call Server Variants
CoRes Co Resident Call Server
Single Call server – No redundancy
Co resides with Sig Server on Linux Platform
VxWorks Emulator VxEll
CPPM / CPDC / CPMG / COTS
SA Standard Availability Call Server
Single Call server – No redundancy
CPPM hardware only
VXWorks
HA High Availability Call server
Dual Call Server CP0 / CP1 (Active and Inactive CS)
CPPM & Pentium IV hardware
VxWorks
Campus Redundancy – CP0 & CP1 in different locations (~40Km)
High Speed Pipe (HSP) Connects Call Servers together
Synchronises Memory and Fixed Media Device (FMD)
HS High Scalability
"Clustered " HA call servers hence only CPPM – up to 150,000 users
20

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

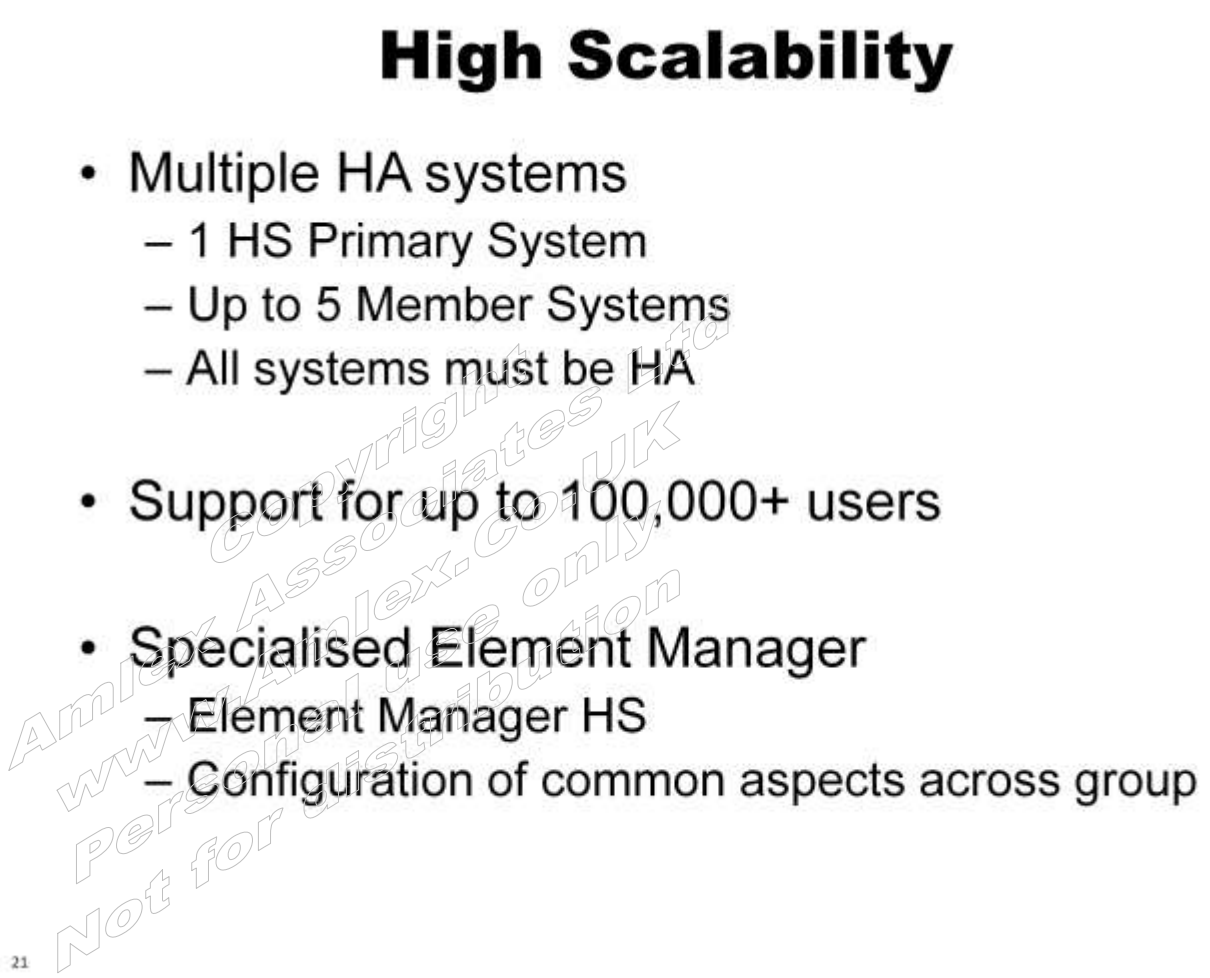
_____

_____

High Scalability provides a new platform for very large systems. It combines up to 6 High Availability systems, one the Primary and the rest as Members.

A new Element Manager HS is used to provide configuration of common elements across the systems.

Inter-Nodal traffic is transported using SIP and an Internal dial plan established for this. Common areas of the database are “Shared” from the Primary to “Member” call servers using a Specialised HS Element Manager.


High Scalability
• Multiple HA systems
– 1 HS Primary System
– Up to 5 Member Systems
– All systems must be HA
• Support for up to 100,000+ users
• Specialised Element Manager
– Element Manager HS
– Configuration of common aspects across group
21

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____
_____
_____
_____

Pentium IV processors are housed in their own chassis (Two shown in the picture).

The chassis has three slots however the top slot is not used (used for Drive carrier card for Pentium II systems). The Middle slot carries the CPU card itself whilst the lower slot has the Utility card.

The Utility card has the DIP switches used to tell the system which processor is CP0 and which CP1. It also carries the system security Dongle.

Pentium IV – Call Server

- Pentium IV Processors
  - Redundant Only (High Availability HA)
  - PKG 410 in Keycode
  - Separate Chassis
  - Use Utility Card
    - CPU0 / CPU1 (DIP s/w)
    - Security Device (Dongle)
- Campus Redundancy
  - CPU's up to 40Km apart
- Upgrade Only
  - Not available for new purchase

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

22

Notes

_____

_____

_____

_____

Common Platform Pentium Mobile (CPPM) call servers are a single board solution and can be used for Standard availability (SA) & High availability (HA) systems. The security device is carried on the board itself and the “Side “ information is set in the bios of the board.

As a call server, the CPPM has a 1GB Compact flash as its FMD (fixed Media Device – hard drive) and uses a 512 Mb compact flash for software installation, RMD (Removable Media Device). To set the board to boot from the compact flash the onboard switch is set to position 1.

CPPM devices use a standard IPE slot in a Media Gateway but only receive power from it and connect to the console port through it. They do not communicate with other cards in the chassis or cabinet across the backplane.

A High Availability CPPM based system will support a combination of up to 50 Media gateways or 40000 IP Sets.

CPPM - Call Server

- Common Platform Pentium Mobile
  - 1Gb DDR RAM Exp to 2Gb
  - Compact Flash RMD
  - 3 x Ethernet ports
  - 2 x SDI Ports
  - Used for Call Server & Sig Server
- Call Server
  - High or Standard Availability
  - Security Device On-Board
  - No Utility Card Required
  - 1Gb Compact Flash FMD
- Resides in any slot in Cabinet or Chassis except Slot 0
- Dedicated slot in MG1010

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

23

Notes

_____

_____

_____

_____

Common Platform Pentium Mobile (CPPM) Linux server can be used as a Signalling Server or Co-resident Call server or merely a Primary or Backup UCM.

The CPPM Linux server is the same board as the call server but it is now equipped with at least a 40Gb laptop hard drive instead of the 1Gb compact flash, 2Gb or RAM and the onboard switch is set to position 2 to ensure it boots from the hard disk.

CPPM devices use a standard IPE slot in a Media Gateway but only receive power from it and connect to the console port through it. They do not communicate with other cards in the chassis or cabinet across the backplane. If you are using a CPPM sig server in a 1000M it must be the dual width device to avoid fouling other cards.

Single width CPPM for use in Media gateways :-
NTDW61

Dual width CPPM for use in CS1000M :-
NTDW66

Single width Metal faceplate CPPM for use in Media gateways 1010 :-
NTDW99

CPPM – Linux Server

- Common Platform Pentium Mobile
  - 2Gb RAM
  - 40GB or larger Hard disk
- Co Resident Call Server option.
  - Dongle Required
  - Upgrade Only
- All UCM Options
  - Primary/Backup/Member
- Resides in any slot in Cabinet or Chassis except Slot 0
- Dedicated slot in MG1010

24

Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

CPMG

The CPMG card combines the functionality of both Linux Server and Media Gateway Controller.

This gives a single slot option for a CoRes Call server for small systems.

The card is available with either 32 or 128 DSP's which are fixed on the board and therefore not upgradeable.

Linux Server is accessed using the TTY ports on the front of the card presented as RJ45 sockets. A special adaptor (RJ45 to 9 pin D type) is required to connect to the serial port .

The Media Gateway component is configured as an MGS to the call server. It uses the existing TTY connection via the chassis SDI port thus configuration is completely separate from Linux sever.

The Call server and Media Gateway can have separate internal Ethernet connections and IP addresses but the CPMG has an internal Ethernet switch so connection is automatically achieved between the two devices once the IP addresses are configured.

- Common Processor Media Gateway
  - Media Gateway Controller & Linux Server on one card
  - Intel 1.2Ghz Tolapai processor
    - 2 Gb RAM
    - 250 Gb SATA hard disk
  - Available with 32 or 128 DSP
    - Fixed on Board not U/G
  - CoRes Call Server System
    - Users Limited by DSP Count
  - Installation from USB stick
  - Uses RJ45 socket on Front of card for CS TTY
    - Specialised adaptor required
    - MGS Uses existing TTY ports

25

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution Copyright

Notes

_____

_____

_____

_____

The CPDC card replaces the CPPM card for Linux applications. The CPPM will no longer be supplied new for Linux CoRes deployments (Upgrades allowed) .

The CPDC will not support VxWorks so is not available for the SA or HA configurations.

The server has no INI or DIP switches for configuration but does have a VGA port on the front of the card.

The card shares the same TTY port cable as the CPPM card.

The CPDC can support the new IP Media Application Services or MAS server. This is a method of providing IP based conferencing tones and announcements.

CPDC

- Common Processor Dual Core
  - IPE Card
  - AMD 1.8Ghz Athlon processor
  - 2 x DDR2 memory slots – 4Gb per slot
  - 250Gb SATA hard disk
- High Capacity Linux Server
  - Installation from USB stick
  - UCM
  - Sig Server
  - NRS
  - CoRes Call Server System
  - IP Media Services Role (Exclusive)
- Replaces CPPM for CoRes/Linux deployment
- No VxWorks Call Server

Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

26

Notes

_____

_____

_____

_____

HP, IBM & Dell servers are known as COTS (Commercial of the Shelf) servers. They come with 2 Gb of memory and either one or two hard drives. They have at least 2 Ethernet ports for ELAN & TLAN and run Linux.

The COTS1 servers, HP DL320 and IBM x306 only have a single 80Gb drive as standard and were originally introduced with CS1k Release 5.

The COTS2 servers, Dell R300 and IBM 3350 were introduced with CS1K Release 6 and feature redundancy of Hard disk and power supplies. This makes them an excellent choice as a platform for the Primary UCM.

NOTE:-
The ISP1100 is not supported for Linux and thus cannot be used after Release 5.

1U - Linux Servers

- Rack Mount Option
- COTS1
  - IBM x306
  - HP DL320
  - 2 Gb single 80Gb HD
- COTS2
  - IBM 3350
  - Dell R300
  - HP DL360 G7
  - 2Gb Mirrored 250Gb HD's
  - Optional Dual PSU

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

27

Notes

_____

_____

_____

_____

Either the Chassis or Cabinet can be used for the Media gateway on a CS1000E system.

The Chassis is a 5 slot main unit with an optional 4 slot Expander cabinet. The two are connected using 2 copper cables.

The expander is a part of the main media gateway and only adds the 4 card slots , no other functionality.

Media Gateway

- Chassis or Cabinet form factor
- Chassis
  - Main Unit – MGC + 4 slots (1-4)
  - Expansion – 4 slots (7-10)
- Cabinet
  - MGC + 10 slots
- Media Gateway Controller (MGC)
  - Controls Card slots
  - Communicates with CS
  - 3 SDI Ports
  - Multi Homing option for ELAN & TLAN
  - Always Slot 0

28

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

If using the Media Gateway chassis then the picture shows the relevant ports for connection. The cards in the units will use the 25 Pair connectors to link to the MDF. In a chassis configuration the Main unit & Expander are linked by 2 copper cables.

MGC SDI (Serial Data Interface) ports are connected using the “Triple Cable” these ports are used for the initial configuration of the MGC card itself but once it has been integrated and has registered with the call server they can be configured as further TTY ports on the call server itself for access or CDR collection etc.

The ELAN & TLAN ports on the back of the chassis are the redundant connections for the MGC and mirror the 1E & 2T ports on the faceplate of the card itself. If you are not using multi homing then either connection maybe used. Swapping between these ports is controlled by the MGC itself and is not reliant upon any other network interaction.

Expander Connection

- Chassis & Expander
  - Interconnect with
    - CEMUX & DS-30
- 8 Cards use 25 Pair Connectors to MDF
- SDI Ports from MGC
  - 3 x TTY ports from CS
- ELAN & TLAN
  - Bottom Left on Main Unit
- Bulkhead Ports
  - Connect to sockets Bottom right of Main Unit

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

29

Notes

_____

_____

_____

_____

Bulkhead Ports

The Bulkhead ports on the Media Gateway are used purely for connecting to the back of the chassis. They act like an extension cable only and can be used by any connection ELAN or TLAN on the system.

The DIP switches are used to set the ring frequency etc and should be set according to the relevant NTP country information.

- Bulkhead Ports
  - Connect to sockets on rear
- Power switch on front of Chassis
- DIP Switches
  - for setting Ring Frequency etc

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

30

Notes

_____

_____

_____

_____

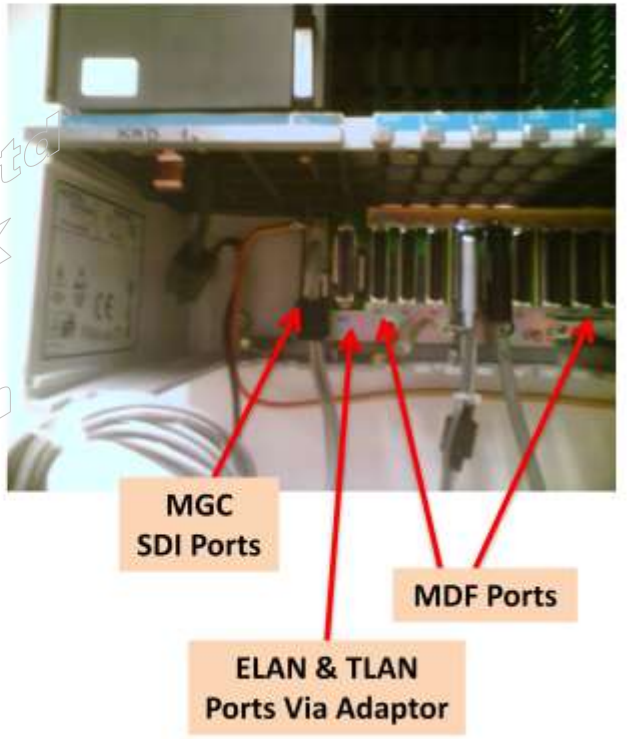
The Media Gateway cabinet is similar in requirements to the chassis as far a card connections go but he location of connectors is at the bottom of the cabinet as shown here.

The SDI ports are connected again using the triple cable, and the ELAN & TLAN redundant ports are connected using a specialised adaptor similar but not the same as the Media card adaptor.

This allows for the duplication of the 1E & 2T ports on the faceplate of the MGC itself in slot 0.

Media Gateway Cabinet

- Cards use 25 Pair Connectors to MDF
- SDI Ports from MGC
  - 3 x TTY Ports from CS
- ELAN & TLAN Ports
  - Dual Homed ports Via Adaptor Duplicate ELAN & TLAN on MGC Facelate



Amlex Associates Ltd
www.amlex.co.uk
Copyright
Personal use only
Not for distribution

31

Notes

_____

_____

_____

_____

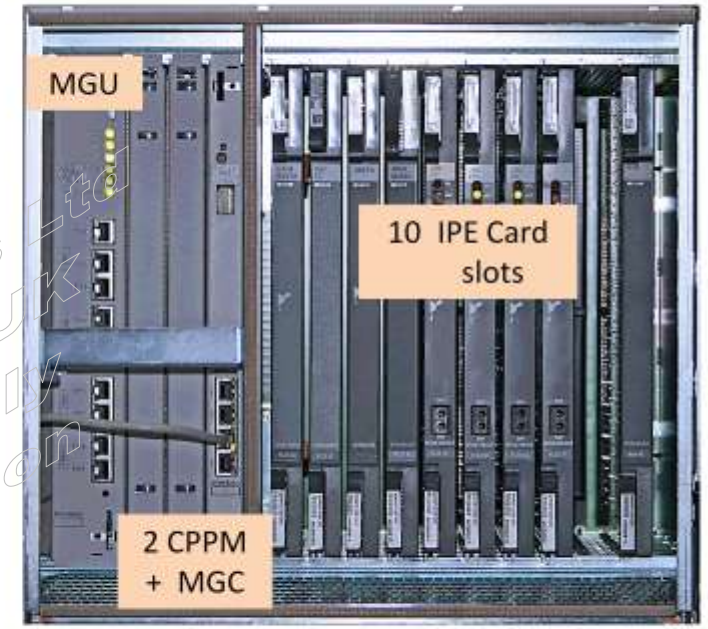
Media Gateway 1010

The Media Gateway 1010 is a rack mounted chassis which has provision for up to 10 IPE cards. In addition it can house two CPPM cards in dedicated slots thus not using up IPE slots.

The chassis uses a standard MGC card but has an additional MGU (Media Gateway Utility card) which allows access to the console ports of the MGC and CPPM cards installed as well as supporting the redundant ELAN and TLAN ports of the MGC.

In addition to increase resilience of the chassis it has a redundant power supply and triple fan units. This addresses one of the primary concerns over the standard 5 slot Media Gateway chassis.

- MG1010
  - 10 IPE Card slots
  - 2 CPPM/CPDC Card slots
  - 1 MGC
    - Standard Conrtroller
  - 1 MGU
    - Dedicated 1010 Utility Card
    - Hot Swap
- Redundancy
  - Dual PSU
  - Triple Fan



Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

32

Notes

_____

_____

_____

_____

Media Gateway Controller

Uses slot 0 in Media Gateway and Is keyed so it wont fit in any other slot.

The MGC uses a Gold Image to boot from and connect to the call server, thus no software has to be installed on the card. Updates are downloaded from CS and stored on the 128Mb Compact flash.

The MGC has 3 SDI ports on the board which are presented on the triple cable from the port on the cabinet or chassis. The first port is used to configure the card initially but after that they can be configured as extra TTY ports for the call server.

The MGC has space for 2 DSP daughter boards which come as either 32, 96 or 128 port boards.

The 4 digit display on the front of the card displays the LOOP & SHELF when it is connected to a call server.

At boot up it reports its self test BOOT, POST (Power on self test), PASS (Pass self test), LOAD (Application Loading). In the event of an error it will display Exxx where xxx is the error number.

- MGC Card
  - 128 Mb Compact Flash
  - No Software load
    - Uses Gold Image
    - Stores Updates on Compact Flash
  - Option for 2 DSP Daughter Boards (Media Cards)
  - Multi-Homing Option
    - Pass through ports CE CT
    - Dual ELAN & TLAN ports
- Always SLOT 0

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

33

Notes

_____

_____

_____

_____

The addition of the 128 port DSP card increases the number of TDM/IP calls that can be supported using on the MGC card slot. From Rel 5 when the MGC was first introduced it was available with both a 32 and 96 port DSP card and the card could e configured with both a 32 and 96 port card to achieve 128 ports in total.

This can now be extended to 160 ports by using a 128 and 32 port card.

In the PRI gateway two DSP 96 or DB 128 cards can be used to create a non blocking environment.

In this configuration the system must have the Package 418 enabled to function correctly.

DTR's can now also be created on card 0 to allow for the use of the DB 128 card.

128 Port DSP card

- DB 128 card increases DSP resources
- When using two DB 96 or DB 128 on MGC
  - Package 418 Required
- DTR can be configured on card 0 as well as 14 & 15
  - e.g. DB 128 Position 1 – DTR configured on 0 & 15

DSP Card	DSP Position	Configured Cards
DB 32	1	11
DB32	2	0
DB 96	1	11, 12, 13
DB 96	2	0, 9, 10
DB 128	1	11, 12, 13, 14
DB 128	2	0, 9, 10, 15

34

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

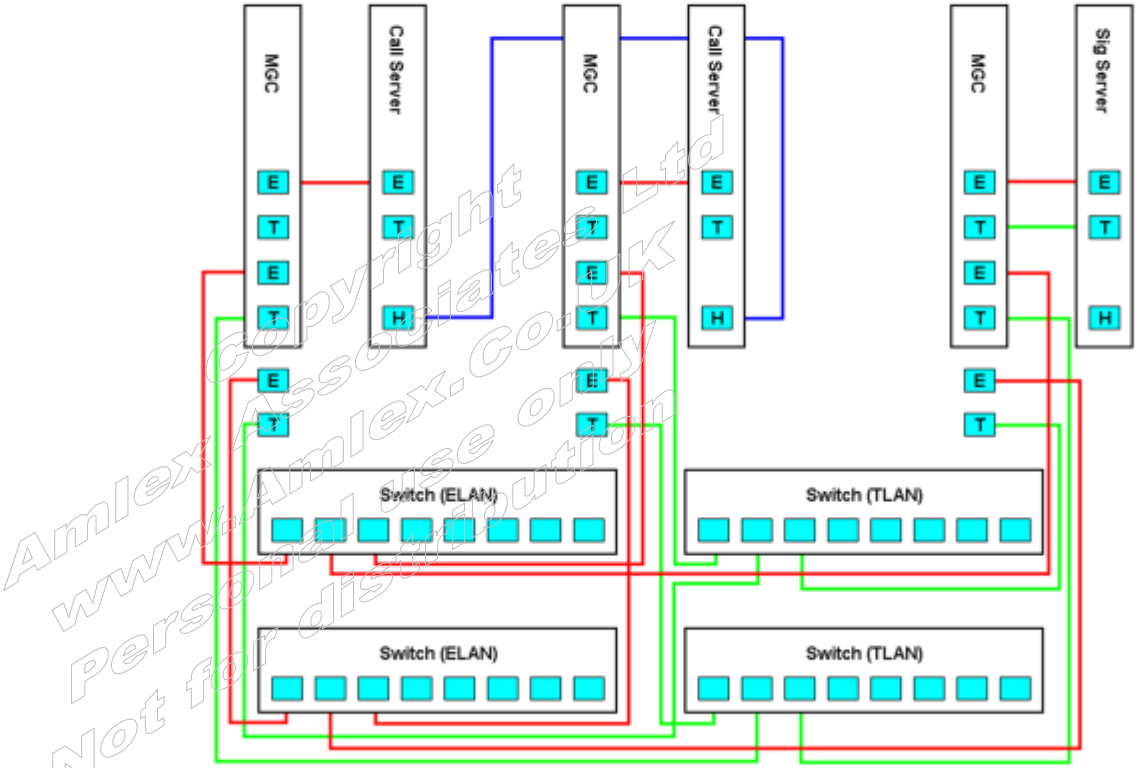
MGC Dual Homed Redundancy

The LAN connections for the system are important and in order to maximise the redundancy of the switch you can take advantage of the multi homing aspects of the MGC cards.

The diagram above shows 3 media gateways schematically and their MGC cards. These are connected to redundant ELAN & TLAN Ethernet switches via the front faceplate and “rear” redundant ports. This allows the MGC to continue to function even if one of the ELAN or TLAN switches fails.

NB Note that the interconnection between the Ethernet switches has been omitted for clarity.

To fully utilise this redundancy the Call Server ELAN connections have been connected to the network using the pass through ports (CE) on the front of the MGC. Similarly the Sig Server has both ELAN & TLAN connections to CE & CT on the front of its MGC card.



Amlex Associates Ltd Copyright www.Amlex.Co.Uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Media Card MC 32 s

- Replaces existing VGMC Media card
  - 32 Ports TDM - IP Conversion
  - IPE Format Card
    - Fits 1000M or Media Gateway IPE slot
- Adds SRTP to media card
  - Secure Voice
- Uses BOOTP to obtain IP information

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

36

The Media Card 32 S provides TDM to IP conversion as did its predecessor the VGMC (Voice Gateway Media Card) . However it has the additional functionality to encrypt the voice media using Secure Real Time Protocol (SRTP).

This card can be used where there is no opportunity to use the DSP daughter boards of a MGC in a CS1000M configuration where there are no Media Gateways at all.

It is configured as a part of the IP telephony node but no longer runs TPS as it did in Release 5.

The ELAN & TLAN connections for the card are achieved using a specialised adaptor which plugs into the 25 pair connector for the card. The Ethernet port on the faceplate is currently unused.

Notes

_____

_____

_____

_____

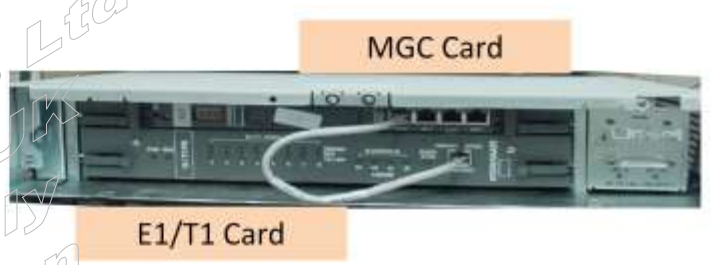
PRI Gateway

The dedicated PRI gateway is a 19”rack chassis with two cards installed. A single Media Gateway controller and an 8 span PRI card. The Quad PRI card is expanded to from 4 to8 circuits using an add on daughter board.

The system is initially programmed via a serial connection to assign IP addressing and subsequently through its own Web interface.

To prevent blocking the MGC card can have two 96 port or 128 port DSP boards installed on it (Requires package 418).

- 2 U Chassis
  - MGC
  - 4 + 4 PRI Spans
  - 4 Downloadable DCH
- Supports
  - 2 x 96 or 128 DSP
  - Cards 0, 9, 10, (15)
  - Cards 11,12,13, (14)



Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

37

Notes

_____

_____

_____

_____

MG XPEC

The MG XPEC is a new controller that allows an existing IPE shelf from a Single or Multi group switch to be re-used in a CS1000E environment.

The card is effectively a Dual MGC and replaces the shelf controller creating a Dual MGC which can be integrated within a CS1000 architecture.

- XPEC Controller for CS1000E
  - IPE Shelf
- Allows System Migration
  - SG & MG systems to CS1000
- Dual MGC configuration
  - Turns IPE shelf into Two Media gateways.
- Clock Controller link for DECT

38

Amlex Associates Ltd Copyright www.Amlex.Co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

3. Building an SA or HA System

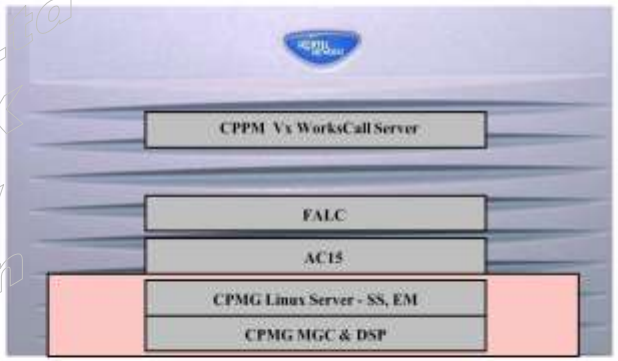
For high numbers (> 1000) of Users on a CS1K system the Call server options are a VxWorks based Standard Availability or High Availability system . (High Scalability systems are based on multiple HA configurations).

The VxWorks installation must be carried out directly to the server itself, no deployment options are available from the UCM. The server will of course require a UCM, Signalling Server and Element Manager which are provided by the CPMG card in the example shown (not a typical configuration).

As the VxWorks Call Server has initially no relationship to the Linux server, unlike a CoResident option, it must have its IP addressing added after installation and be assigned to the SS & EM during their deployment.

As the CPMG is not acting as a Call Server in this instance it will not require a Dongle for installation.

- SA & HA call Servers only run on VxWorks
- Must have Linux Server for Element Manager & Signalling Server
- IP addressing set in LD 117 after installation



Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

39

Notes

_____

_____

_____

_____

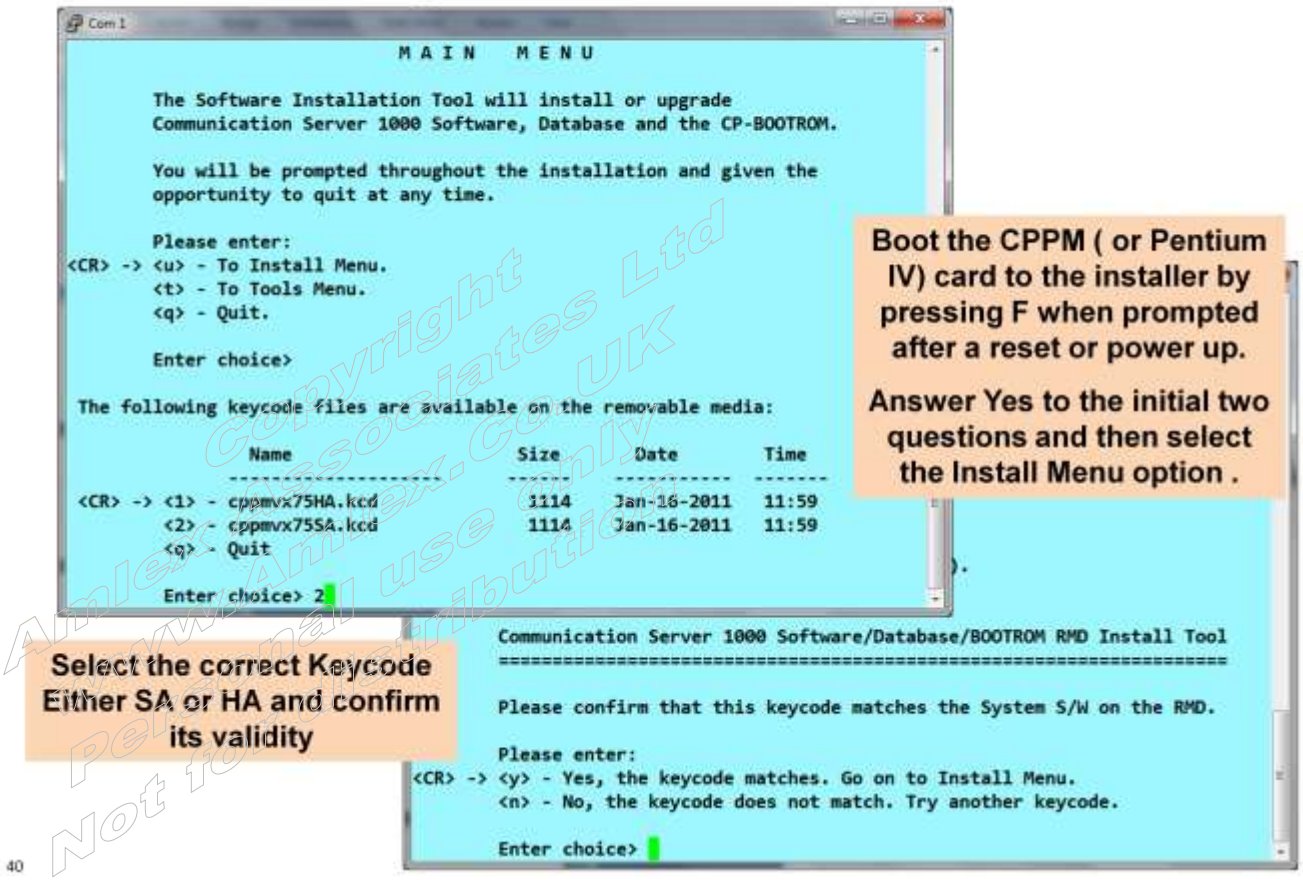
Installing VxWorks Call Server

The installation of the VxWorks Call Server is still carried out using a specially prepared Compact Flash (CF) card inserted in the RMD (Removeable Meia Device) slot on the front of the card.

As the system boots strike the F key when prompted to boot from the Faceplate CF and if the system has been used before (i.e. There are system files on the FMD (Fixed Media Device) type F again when prompted to select the CF boot.

Proceed with the installation typing Y to the first two questions until you are offered the INSTALL MENU selection.

The Next prompt will be to identify the Keycode from a list select the appropriate item (HA for our purposes). The system then checks this is a valid option and asks for confirmation.


Com 1
MAIN MENU
The Software Installation Tool will install or upgrade
Communication Server 1000 Software, Database and the CP-BOOTROM.
You will be prompted throughout the installation and given the
opportunity to quit at any time.
Please enter:
<CR> -> <u> - To Install Menu.
<t> - To Tools Menu.
<q> - Quit.
Enter choice>
The following keycode files are available on the removable media:
Name Size Date Time
<CR> -> <1> - cppmvx75HA.kcd 1114 Jan-16-2011 11:59
<2> - cppmvx75SA.kcd 1114 Jan-16-2011 11:59
<q> - Quit
Enter choice> 2
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
Please confirm that this keycode matches the System S/W on the RMD.
Please enter:
<CR> -> <y> - Yes, the keycode matches. Go on to Install Menu.
<n> - No, the keycode does not match. Try another keycode.
Enter choice>
Boot the CPPM (or Pentium IV) card to the installer by pressing F when prompted after a reset or power up.
Answer Yes to the initial two questions and then select the Install Menu option .
Select the correct Keycode Either SA or HA and confirm its validity

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

40

Notes

_____

_____

_____

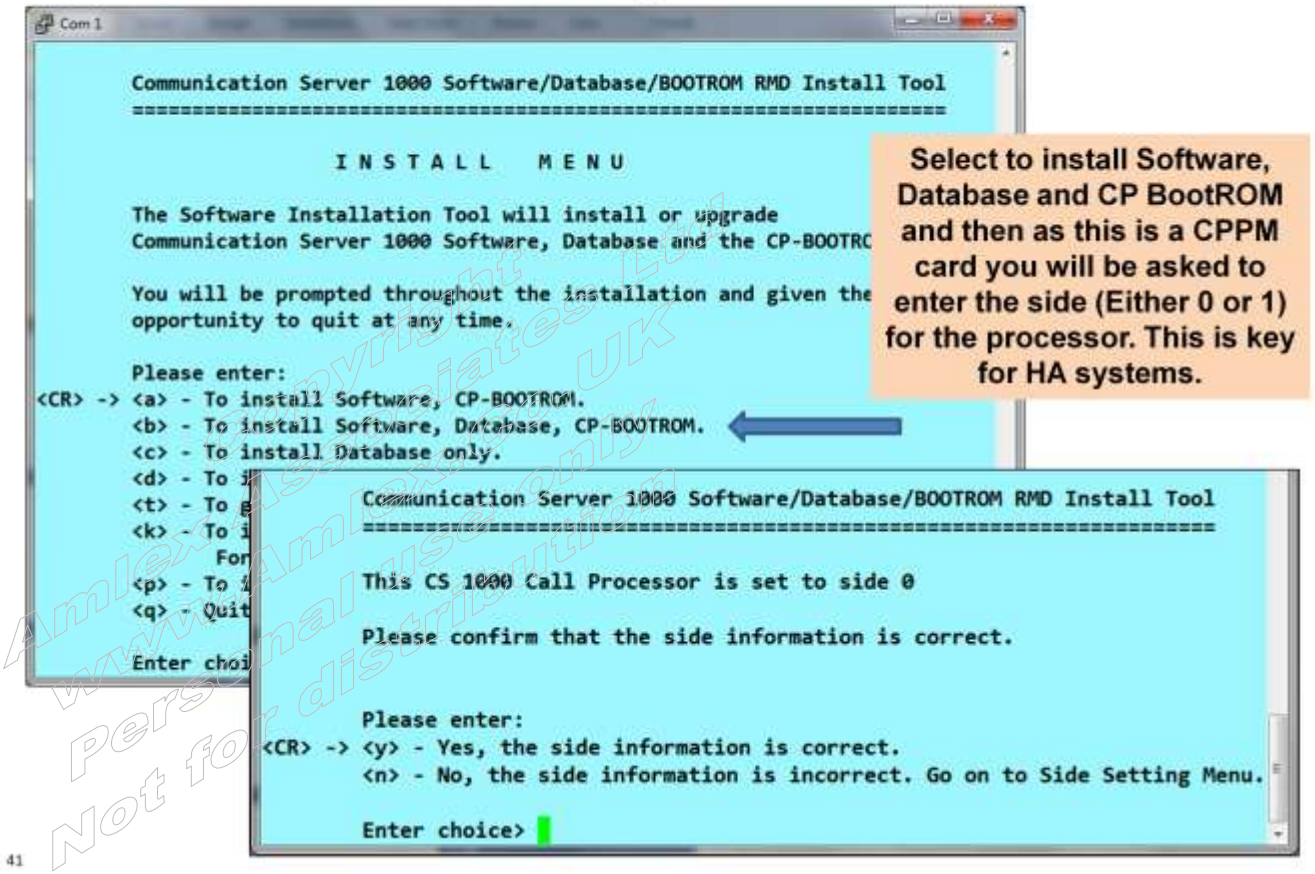
_____

Select Install Options & CS Side

The INSTALL MENU will then be displayed and the appropriate selection made. We are using option B to install the Software, Bootrom and a Database.

The system will then check the SIDE setting of the call server. For an HA (High Availability) system the processors need to be defined as 0 or 1 i.e. They must be unique to allow the duplication of their running configurations. On the CPPM card this is held in the BIOS and is set during install.

For an SA (Standard Availability) system set the side to 0.


Com 1
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
INSTALL MENU
The Software Installation Tool will install or upgrade
Communication Server 1000 Software, Database and the CP-BOOTRC
You will be prompted throughout the installation and given the
opportunity to quit at any time.
Please enter:
<CR> -> <a> - To install Software, CP-BOOTROM.
<b> - To install Software, Database, CP-BOOTROM.
<c> - To install Database only.
Select to install Software, Database and CP BootROM and then as this is a CPPM card you will be asked to enter the side (Either 0 or 1) for the processor. This is key for HA systems.
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
This CS 1000 Call Processor is set to side 0
Please confirm that the side information is correct.
Please enter:
<CR> -> <y> - Yes, the side information is correct.
<n> - No, the side information is incorrect. Go on to Side Setting Menu.
Enter choice>

Notes

_____

_____

_____

_____

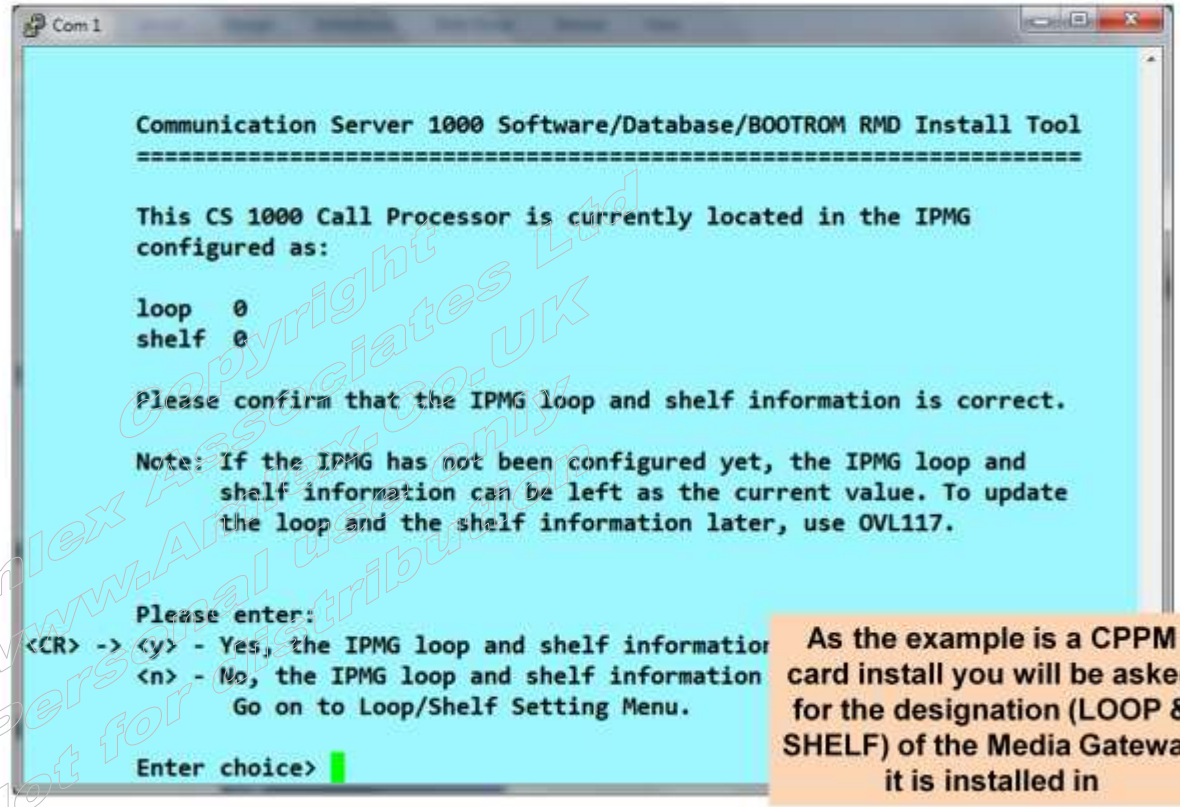
Copyright Amlex Associates Ltd

Define the Media Gateway Location

As the CPPM is installed in a Media Gateway card slot it will then ask which one. This information is only used by the inventory command in LD 117 and does not affect the system performance if set incorrectly.

See overlay 117
> CHG LCL Loop Shelf

Add the LOOP and SHELF designation for the Media Gateway that the card is installed in. The Slot number will be picked up automatically.


Com 1
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
This CS 1000 Call Processor is currently located in the IPMG configured as:
loop 0
shelf 0
Please confirm that the IPMG loop and shelf information is correct.
Note: If the IPMG has not been configured yet, the IPMG loop and shelf information can be left as the current value. To update the loop and the shelf information later, use OVL117.
Please enter:
<CR> -> <y> - Yes, the IPMG loop and shelf information
<n> - No, the IPMG loop and shelf information
Go on to Loop/Shelf Setting Menu.
Enter choice>

As the example is a CPPM card install you will be asked for the designation (LOOP & SHELF) of the Media Gateway it is installed in

42

Notes

_____

_____

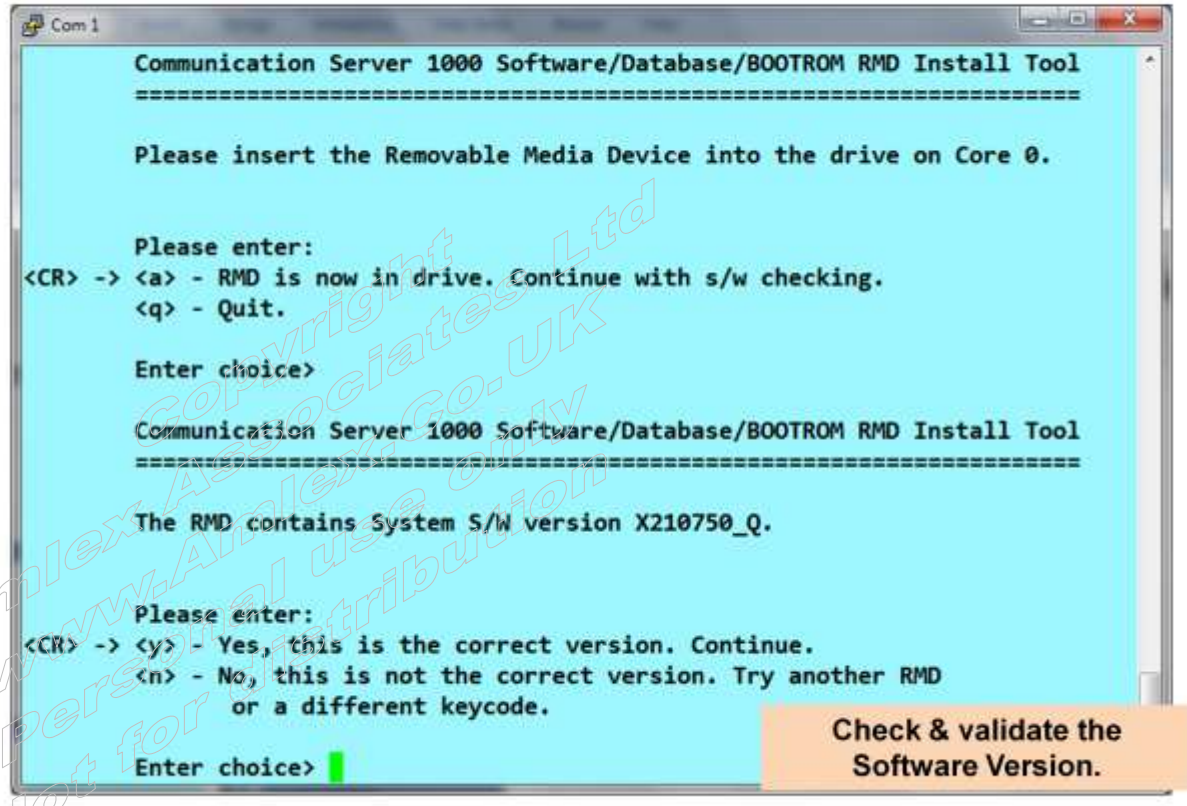
_____

_____

Copyright Amlex Associates Ltd

Check Software Version

The system is now ready to install and prompts to check the release of software to be installed. This is the software on the Compact Flash installer itself hence the reference to RMD.


Com 1
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
Please insert the Removable Media Device into the drive on Core 0.
Please enter:
<CR> -> <a> - RMD is now in drive. Continue with s/w checking.
<q> - Quit.
Enter choice>
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
The RMD contains System S/W version X210750_Q.
Please enter:
<CR> -> <y> - Yes, this is the correct version. Continue.
<n> - No, this is not the correct version. Try another RMD
or a different keycode.
Enter choice>
Check & validate the Software Version.

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

43

Notes

_____

_____

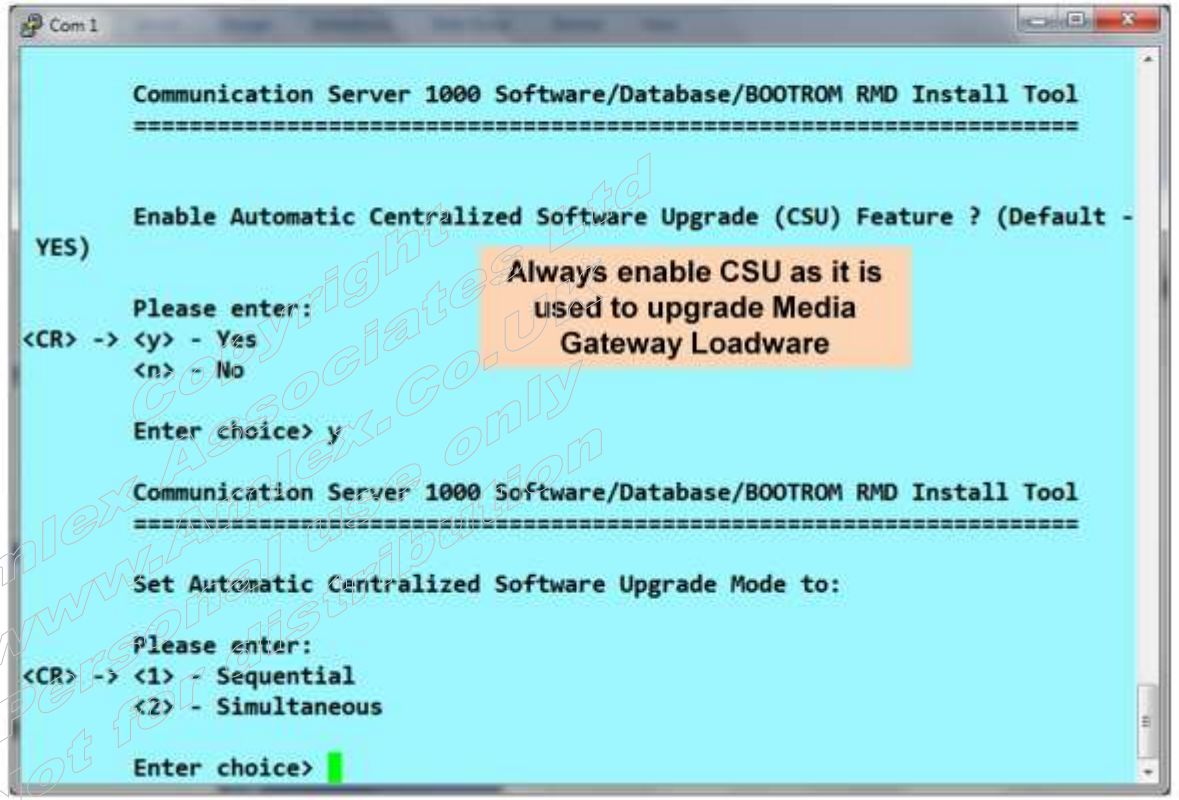
_____

_____

Enable Centralised S/W Upgrade

The installer will now prompt to check if Centralised Software Upgrade should be used. This is the mechanism that allows Media Gateways to download Loadware upgrades automatically and should be enabled.

The second question is whether this should be done Sequentially or Simultaneously i.e. One at a time or all together.


Com 1
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
Enable Automatic Centralized Software Upgrade (CSU) Feature ? (Default - YES)
Please enter:
<CR> -> <y> - Yes
<n> - No
Enter choice> y
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
Set Automatic Centralized Software Upgrade Mode to:
Please enter:
<CR> -> <1> - Sequential
<2> - Simultaneous
Enter choice>
Always enable CSU as it is used to upgrade Media Gateway Loadware

Amlex Associates Ltd Copyright www.Amlex.Co.Uk Personal use only Not for distribution

44

Notes

_____

_____

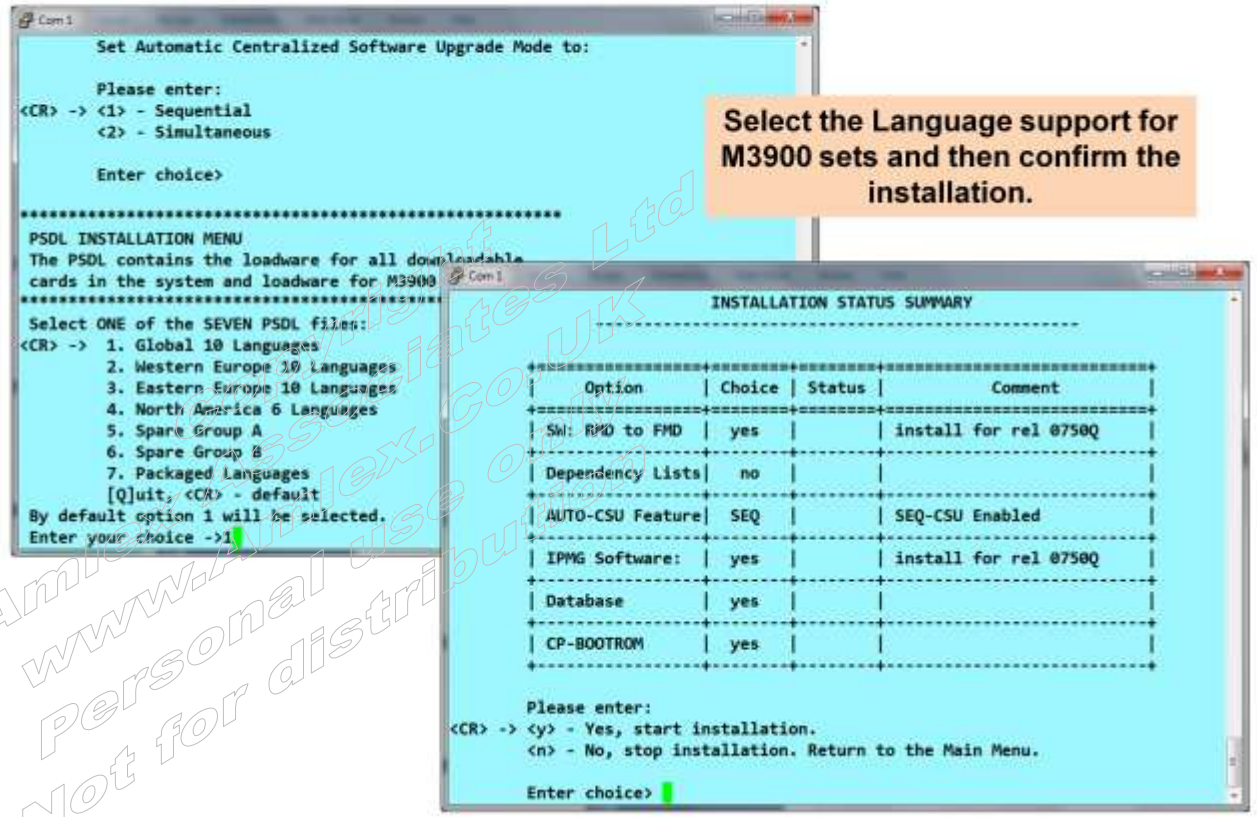
_____

_____

Copyright Amlex Associates Ltd

Select language Support

One of the last question requests the Languages to be supported by the system. You are then presented with a summary and asked if the installation should proceed.


Set Automatic Centralized Software Upgrade Mode to:
Please enter:
<CR> -> <1> - Sequential
<2> - Simultaneous
Enter choice>
PSDL INSTALLATION MENU
The PSDL contains the loadware for all downloadable
cards in the system and loadware for M3900
Select ONE of the SEVEN PSDL files:
<CR> -> 1. Global 10 Languages
2. Western Europe 10 Languages
3. Eastern Europe 10 Languages
4. North America 6 Languages
5. Spare Group A
6. Spare Group B
7. Packaged Languages
[Q]uit, <CR> - default
By default option 1 will be selected.
Enter your choice ->1
Select the Language support for M3900 sets and then confirm the installation.
INSTALLATION STATUS SUMMARY
Option | Choice | Status | Comment
SW: RPD to FMD | yes | | install for rel 0750Q
Dependency Lists | no | |
AUTO-CSU Feature | SEQ | | SEQ-CSU Enabled
IPMG Software: | yes | | install for rel 0750Q
Database | yes | |
CP-BOOTROM | yes | |
Please enter:
<CR> -> <y> - Yes, start installation.
<n> - No, stop installation. Return to the Main Menu.
Enter choice>

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

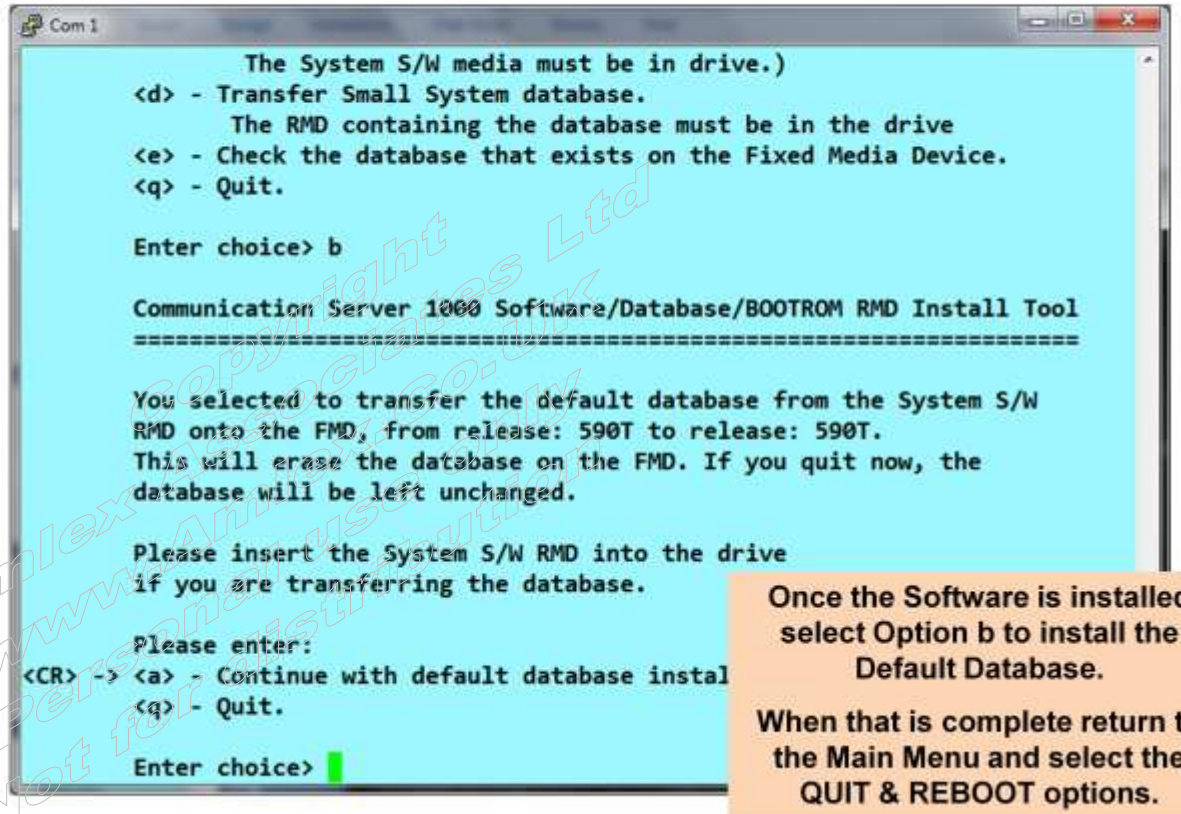
Once the software has been installed the system will return a prompt to continue and request the database to be installed.

On the database selection Menu we have chosen option b the Default Database although an existing database could be used or a small system database converted (Option d). Once selected the system asks for confirmation and then proceeds.

Once this is complete the system returns to the main menu where you should select the Quit option using the prompts on the screen to Quit the installer and Reboot the machine rather than using the Reset button on the card itself.
When configuring a HA system you will repeat the install on the second Call Server ensuring the High Speed Pipe is connected between the two when they reboot. This should allow them to JOIN together with one becoming the ACTIVE call server while the other runs in STANDBY mode.
Once the system boots you will be able to login using the CS1K account "admin2 with the password "0000".

NOTE: The STANDBY CS will not allow a login when joined to the ACTIVE CS. The overlays will only be available on the standby when the systems are SPLIT (LD 135), this is to allow upgrade etc."

Select the Default Database


Com 1
The System S/W media must be in drive.)
<d> - Transfer Small System database.
The RMD containing the database must be in the drive
<e> - Check the database that exists on the Fixed Media Device.
<q> - Quit.
Enter choice> b
Communication Server 1000 Software/Database/BOOTROM RMD Install Tool
You selected to transfer the default database from the System S/W
RMD onto the FMD, from release: 590T to release: 590T.
This will erase the database on the FMD. If you quit now, the
database will be left unchanged.
Please insert the System S/W RMD into the drive
if you are transferring the database.
Please enter:
<CR> -> <a> - Continue with default database instal
<q> - Quit.
Enter choice>

Once the Software is installed select Option b to install the Default Database.

When that is complete return to the Main Menu and select the QUIT & REBOOT options.

46

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

The call server is configured through both the command line interface (CLI) as well as the Element Manager (EM).

The command line is based on “Overlays” or “Loads” and to interact with the system you need to be in the correct “Load” (LD) or “Overlay”.

To login type “LOGI” (Not case sensitive) at the prompt, and either add the username you wish to use on the same line or hit enter for the USERID prompt. Once the Username is input the system will then request a password.

Once logged in to the CLI you change “Overlays” by typing LD and the number of the overlay you require. You must exit an overlay before you can enter another and this is done by typing ****.

There are a few lesser known commands that can be very helpful shown on the right. These allow you to use a limited set of online help and to look up error codes that appear without exiting the overlay.

LON & LOF allow you to backspace in the command line !!

4. Command Line interface

Call Server 1000 and Meridian1 use an Overlay structure
90% of operations can be achieved in CLI

- Login
  - >logi “Username”
  - >pass “Password”
- To Load Overlay
  - LD 117
- To Repeat a Prompt
  - *
- To return to REQ prompt
  - **
- To Exit Overlay
  - ****
- To Logout
  - LOGO
- To look up an error
  - !err sch0101
- To get a list of options when prompt is :
  - Ld 20
  - PRT:
  - TYPE: ?
- Command list in LD 117
  - => ?
- Allow backspace in Overlays
  - >OVL000
  - lon line editor on
  - lof - Line editor off

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

47

Notes

The overlay structure is organised as shown into three primary areas.

System

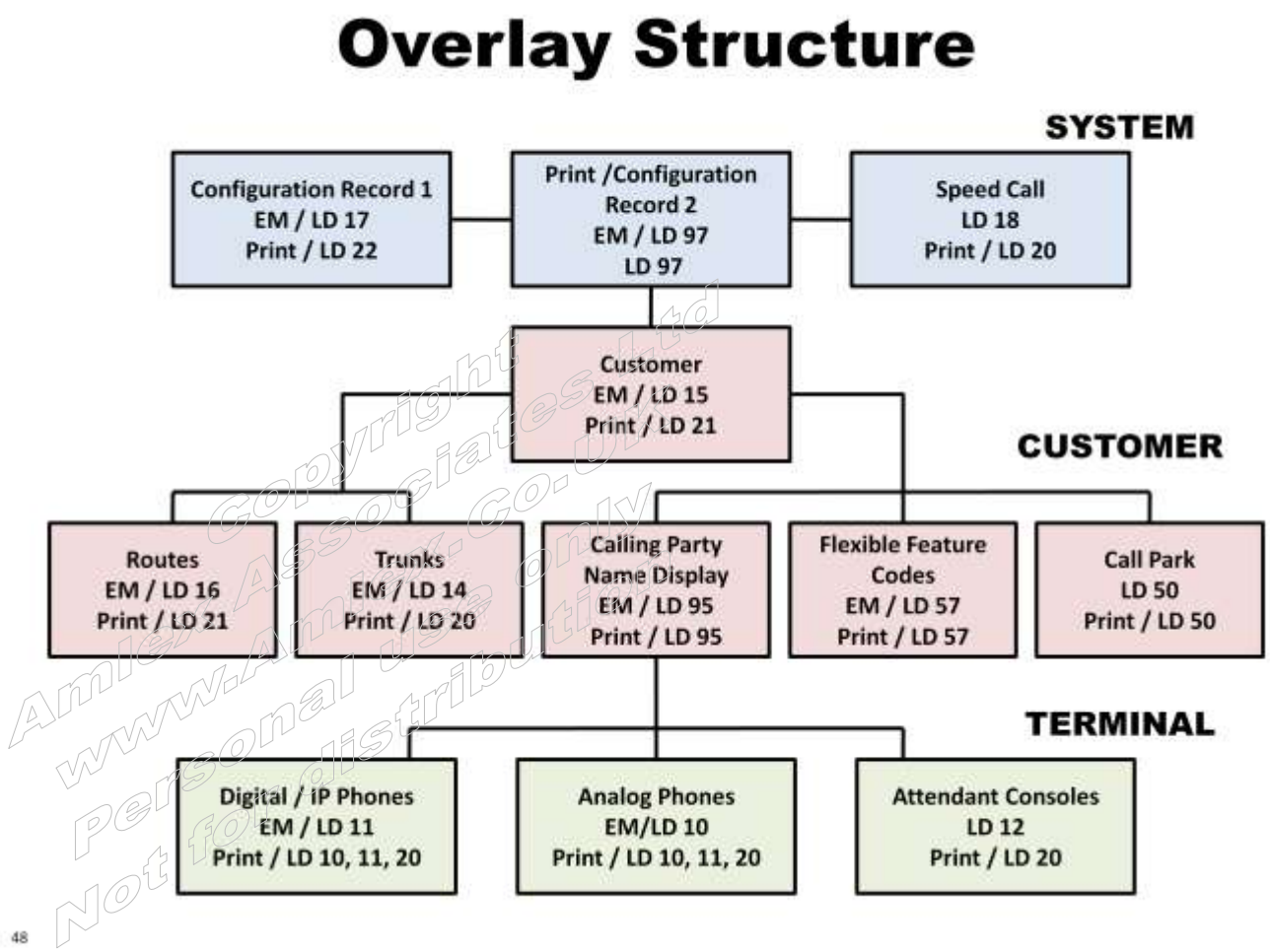
Which deals with the Configuration records, such things as Superloops.

Customer

Most systems only have one customer but there can be several. This deals with the setup of specifics for a particular customer e.g. Routes and Trunks and CPND information.

Terminal or Set

Relates to the actual set properties. Whilst it shows LD 10 & 11 which still exist it is wise to remember that LD 20 is now a linked overlay allowing operations to be carried out for LD 10, LD 11 & LD 32.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

High Availability Checks

As we have a High Availability system we need to check that the system is synchronising correctly between the two cores.

To check the status use the > STAT CPU command in LD 135 . What we should see is a REDUNDANT Status for both the SYSTEM and DISK. This means that both the memory and the disk (FMD) have successfully synchronised allowing us to swap service from one core to the other.

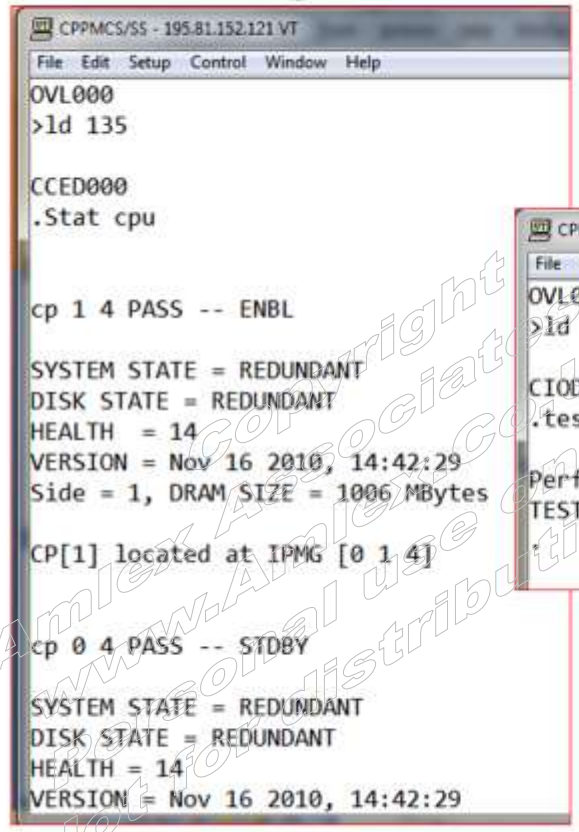
There is also a test which can be run from LS 137

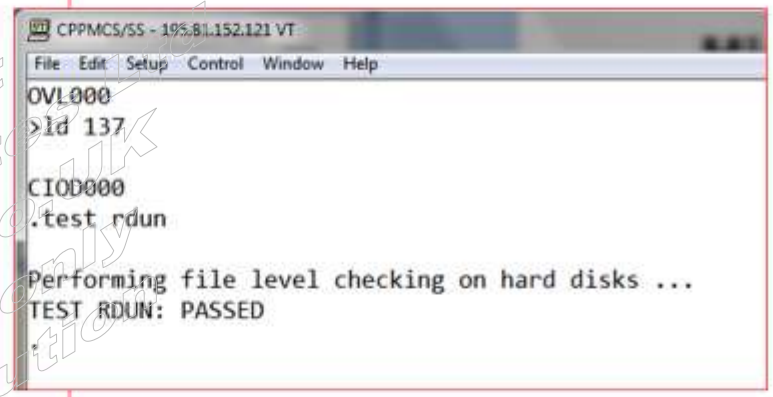
>TEST RDUN

Be patient as the test can take over a minute to run.

To swap the Active and Standby Call servers over we can use the command in LD 135

> SCPU


CPPMCS/SS - 195.81.152.121 VT
File Edit Setup Control Window Help
OVL000
>ld 135
CCED000
.Stat cpu
cp 1 4 PASS -- ENBL
SYSTEM STATE = REDUNDANT
DISK STATE = REDUNDANT
HEALTH = 14
VERSION = Nov 16 2010, 14:42:29
Side = 1, DRAM SIZE = 1006 MBytes
CP[1] located at IPMG [0 1 4]
cp 0 4 PASS -- STDBY
SYSTEM STATE = REDUNDANT
DISK STATE = REDUNDANT
HEALTH = 14
VERSION = Nov 16 2010, 14:42:29



If you've installed a High Availability System check the interaction of the two CPU's

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

49

Notes

_____

_____

_____

_____

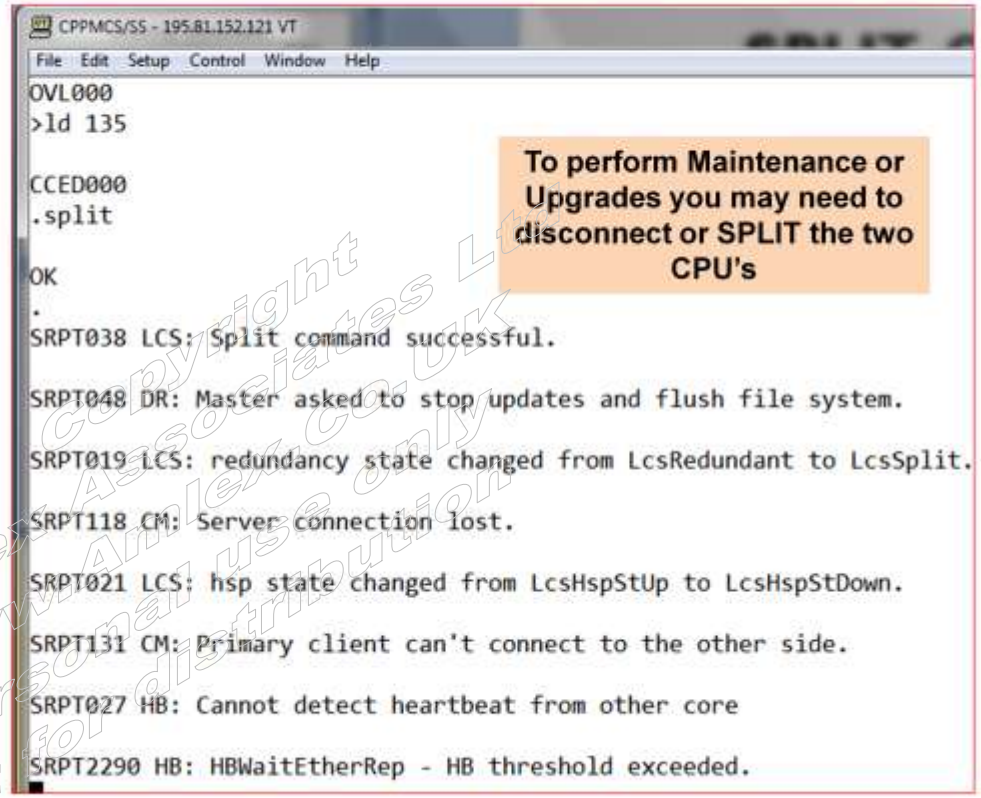
SPLIT Call Servers

In order to upgrade a High Availability system with a minimal loss of service we first need to SPLIT the two cores so we can login to the Standby side.

Once the SPLIT command has been issued you will see the Standby system initialise offering the overlays to login to. (When the two cores are synchronised the standby will be running background tests and the overlays/login will not be available although you can login with PDT).

The ACTIVE core is still processing calls for the system but will no longer try to synchronise with the standby system.

At this point if we were carrying out an upgrade we would now install the upgrade to the Standby system and check its validity before bringing it into service.


CPPMCS/SS - 195.81.152.121 VT
File Edit Setup Control Window Help
OVL000
>ld 135
CCED000
.split
OK
.
SRPT038 LCS: Split command successful.
SRPT048 DR: Master asked to stop updates and flush file system.
SRPT019 LCS: redundancy state changed from LcsRedundant to LcsSplit.
SRPT118 CM: Server connection lost.
SRPT021 LCS: hsp state changed from LcsHspStUp to LcsHspStDown.
SRPT131 CM: Primary client can't connect to the other side.
SRPT027 HB: Cannot detect heartbeat from other core
SRPT2290 HB: HBWaitEtherRep - HB threshold exceeded.
To perform Maintenance or Upgrades you may need to disconnect or SPLIT the two CPU's

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

50

Notes

_____

_____

_____

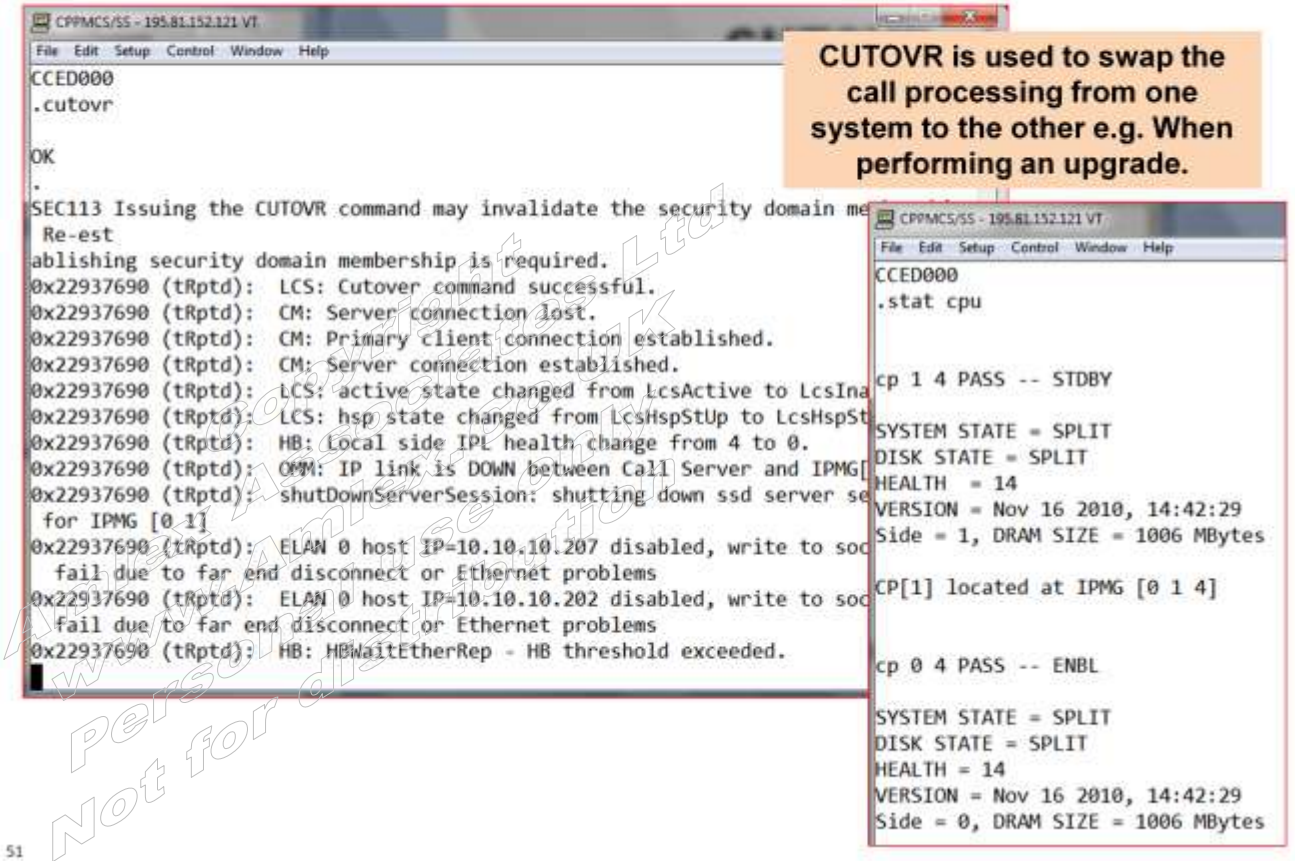
_____

Whilst the command SCPU will swap the call servers when they are joined together when they are SPLIT as we can see here we need to use a different command

> CUTOVR

Issuing the command after upgrading the standby system would bring the upgraded software into service. The cares would still be Split and thus we could then upgrade the second core before joining them back together.

CUTOVR


CPPMCS/SS - 195.81.152.121 VT
File Edit Setup Control Window Help
CCED000
.cutovr
OK
.
SEC113 Issuing the CUTOVR command may invalidate the security domain me
Re-est
ablishing security domain membership is required.
0x22937690 (tRptd): LCS: Cutover command successful.
0x22937690 (tRptd): CM: Server connection lost.
0x22937690 (tRptd): CM: Primary client connection established.
0x22937690 (tRptd): CM: Server connection established.
0x22937690 (tRptd): LCS: active state changed from LcsActive to LcsIna
0x22937690 (tRptd): LCS: hsp state changed from LcsHspStUp to LcsHspSt
0x22937690 (tRptd): HB: Local side IPL health change from 4 to 0.
0x22937690 (tRptd): OAM: IP link is DOWN between Call Server and IPMG[
0x22937690 (tRptd): shutDownServerSession: shutting down ssd server se
for IPMG [0 1]
0x22937690 (tRptd): ELAN 0 host IP=10.10.10.207 disabled, write to soc
fail due to far end disconnect or Ethernet problems
0x22937690 (tRptd): ELAN 0 host IP=10.10.10.202 disabled, write to soc
fail due to far end disconnect or Ethernet problems
0x22937690 (tRptd): HB: HBWaitEtherRep - HB threshold exceeded.
CUTOVR is used to swap the call processing from one system to the other e.g. When performing an upgrade.
CPPMCS/SS - 195.81.152.121 VT
File Edit Setup Control Window Help
CCED000
.stat cpu
cp 1 4 PASS -- STDBY
SYSTEM STATE = SPLIT
DISK STATE = SPLIT
HEALTH = 14
VERSION = Nov 16 2010, 14:42:29
Side = 1, DRAM SIZE = 1006 MBytes
CP[1] located at IPMG [0 1 4]
cp 0 4 PASS -- ENBL
SYSTEM STATE = SPLIT
DISK STATE = SPLIT
HEALTH = 14
VERSION = Nov 16 2010, 14:42:29
Side = 0, DRAM SIZE = 1006 MBytes
51

Notes

_____

_____

_____

_____

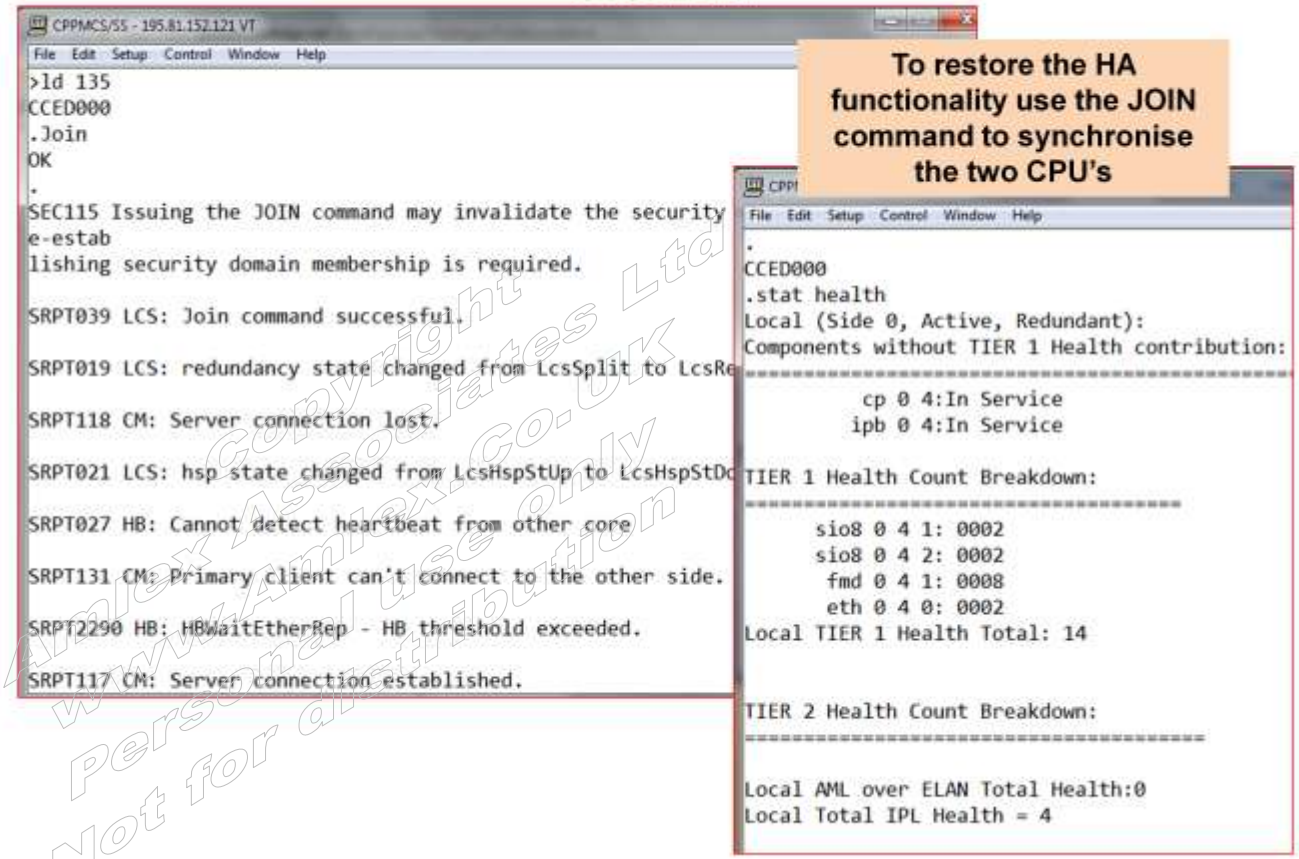
Copyright Amlex Associates Ltd

JOIN

Finally to bring the two cores back together we use the JOIN command from LD 135.

The two CPU's will synchronise and the standby core will resume the background test mode.

Finally we can use the STAT HEALTH command to view the system health which is a number based on the different components of the system and can be used as a gauge of problems with the system.


CPPMCS/55 - 195.81.152.121 VT
File Edit Setup Control Window Help
>ld 135
CCED000
.Join
OK
.
SEC115 Issuing the JOIN command may invalidate the security
e-estab
lishing security domain membership is required.
SRPT039 LCS: Join command successful.
SRPT019 LCS: redundancy state changed from LcsSplit to LcsRe
SRPT118 CM: Server connection lost.
SRPT021 LCS: hsp state changed from LcsHspStUp to LcsHspStDc
SRPT027 HB: Cannot detect heartbeat from other core
SRPT131 CM: Primary client can't connect to the other side.
SRPT2290 HB: HBwaitEtherRep - HB threshold exceeded.
SRPT117 CM: Server connection established.
To restore the HA functionality use the JOIN command to synchronise the two CPU's
File Edit Setup Control Window Help
.
CCED000
.stat health
Local (Side 0, Active, Redundant):
Components without TIER 1 Health contribution:
cp 0 4:In Service
ipb 0 4:In Service
TIER 1 Health Count Breakdown:
sio8 0 4 1: 0002
sio8 0 4 2: 0002
fmd 0 4 1: 0008
eth 0 4 0: 0002
Local TIER 1 Health Total: 14
TIER 2 Health Count Breakdown:
Local AML over ELAN Total Health:0
Local Total IPL Health = 4
52

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Reviewing Configuration Data

The debate rages as to which interface, the CLI or the Element Manager is the easiest to use for configuring and administering the CS1000. In truth it is probably down to how long you have used the system, and the CLI does have a speed advantage if you know exactly what you want to do.

However one area that the Element manager probably wins on is reviewing configuration information as it is presented in web page format with some explanation.

If you want to review configuration information through the CLI then the slide here is a useful one to remember as it points you to the relevant overlay for printing data.

- If it has a TN
  - Print in LD 20
- LD 15 and 16
  - Print in LD 21
- LD 17
  - Print in 22
- Overlays above 22
  - Print in same overlay

Copyright Amlex Associates Ltd www.Amlex.Co.Uk Personal use only Not for distribution

53

Notes

_____
_____
_____
_____

Disabling & Enabling Devices

One thing to always try when devices seem to be okay but still function incorrectly is to DISABLE them and then ENABLE.

Depending on the device you are working on you need to choose the right command as shown here. For a single phone you can use the unit option DISU command in LD 20 (or LD 32). Be aware that on a set the display will remain as if the set is working however you wont be able to pick up a line to dial with.

Whilst you can do this with a single digital set it often better to disable the whole card and then re-enable it. This ensures that it re initialises with the Call Server correctly. Use the DISC for this option.

For replacement or maintenance tasks all cards should be disabled before removal.

Some devices such as PRI , Tone and Conference circuits are addressed as Loops. Thus you use the DISL command to disable these in specific overlays:-
PRI – 60 / TDS – 34 / CONF - 38

- LOOPS / CARDS / UNITS
  - Also certain features DIS / ENL
- LOOP
  - enll (TN) Enable disl (TN) Disable
- CARD
  - enlc (TN) Enable disc (TN) Disable
- UNIT
  - enlu (TN) Enable disu (TN) Disable

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

54

Notes

Copyright Amlex Associates Ltd

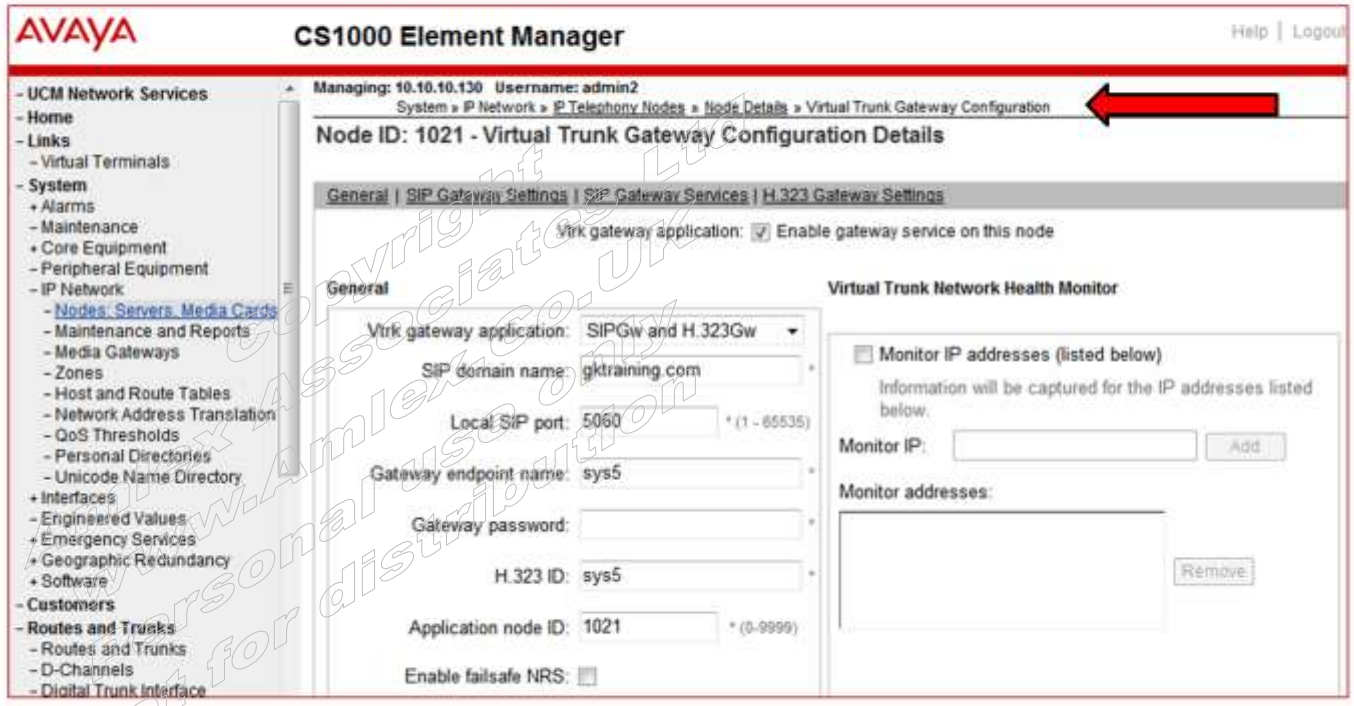
Element Manager

The Element Manager commands in the left hand menu are grouped together to ease navigation.

In addition groups of commands are Sub – Grouped and you will see a + sign where there are more options which have been hidden for clarity.

Here you can see the Main Header **SYSTEM** with the Sub Group **IP NETWORK** expanded to show the options below it. The **NODES, SERVERS, MEDIA CARDS** option had been used to edit the IP Telephony Node.

Note also the “Bread Crumb” trail at the top of the display pane highlighted by the Red arrow. This shows exactly where you are in relation to the Menus and also includes Hyperlinks (Underlined Items) which allow you to move to a different screen without starting back at the initial screen. Note its is not good practice to use the BACK button in the browser as it can lead to display of information which isn’t current.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Not for distribution
Personal use only

Notes

_____

_____

_____

_____

If we choose the default database option on the installation we will need to configure some settings on the call server to ensure it can talk to the Element Manager correctly and is ready for system configuration.

Note that in a CoRes system the IP information will be taken from the Linux base so there is no need for IP Configuration and the commands are disabled in LD 117 for this.

5. Initial Call Server Config

- Configure IP Address & Route
  - LD 117 NEW HOST/ROUTE etc. (Not required for CoRes)
- Add Psuedo TTY's
  - LD 17 PTY
- Remove unwanted items
  - LD 17 CHG CEQU XCT
- Turn on Multi User
  - LD 17 CHG OVLY MULTIUSER ON
- Create a Customer Data Block
  - LD 15 NEW CDB
- Create a Digital Data Block
  - LD 73 NEW DDB
- Create a Bandwidth Zone
  - LD 117 NEW ZONE X
- Configure Virtual Superloops
  - LD 97 CHG SUPL

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

56

Notes

_____

_____

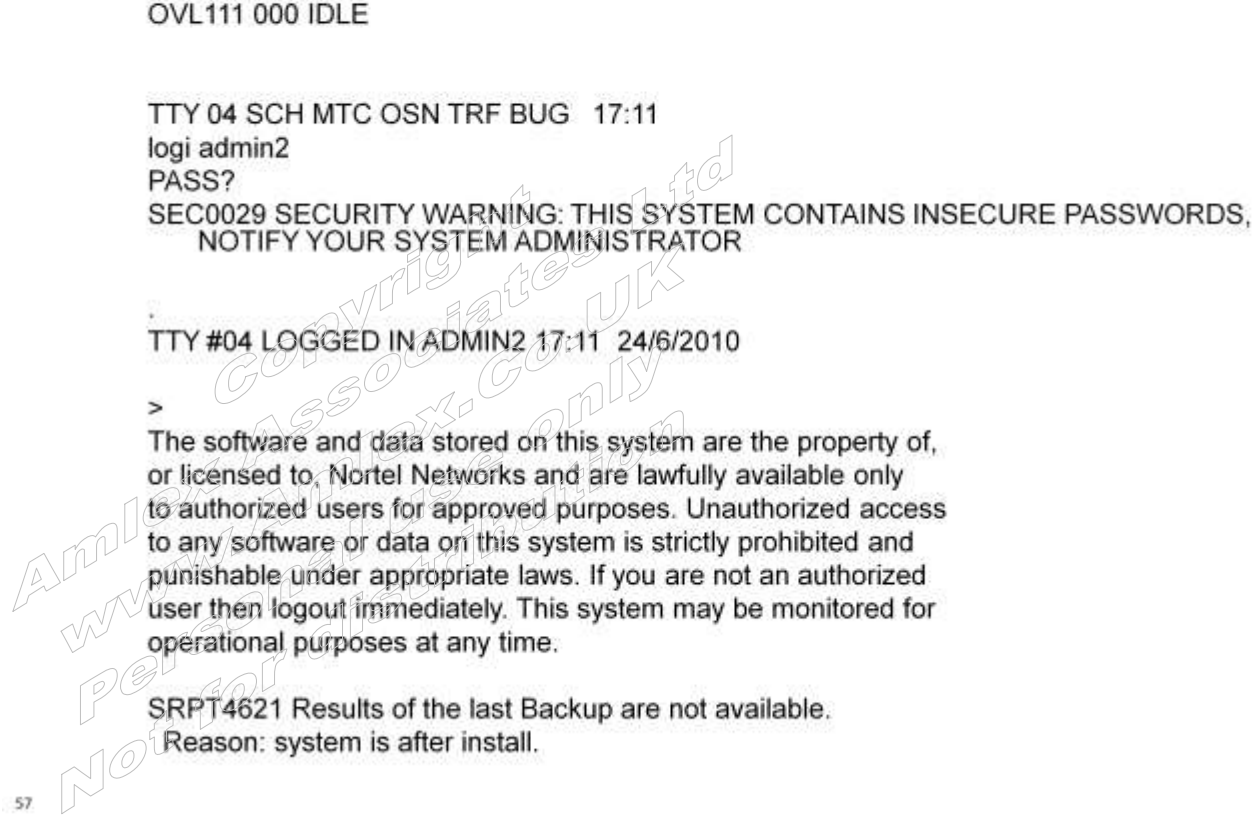
_____

_____

Logging into the Overlays

Here is an example login to the call server overlays using the admin2 account.

It is good to use the admin2 account at this point rather than the admin1 as it has greater privileges and is the only account which can perform security operations which we will need when the Call servers are added to the UCM.


OVL111 000 IDLE
TTY 04 SCH MTC OSN TRF BUG 17:11
logi admin2
PASS?
SEC0029 SECURITY WARNING: THIS SYSTEM CONTAINS INSECURE PASSWORDS,
NOTIFY YOUR SYSTEM ADMINISTRATOR
TTY #04 LOGGED IN ADMIN2 17:11 24/6/2010
>
The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
SRPT4621 Results of the last Backup are not available.
Reason: system is after install.
57

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

The Call Server needs to have an IP address. This ELAN address is set on the call server in load 117.

Dependent on the configuration either one or two addresses may be required. If the system is Standard Availability (SA) then only one address is needed but if it is High Availability (HA - Dual CPU) then an address is required for both CPU's

.

The process is to assign an IP address to a Hostname using the

NEW HOST "Hostname" "IP Address"

command.

The Subnet Mask can be set using the command

CHG MASK "Subnet Mask"

Once this is done the Address is brought into service by command

CHG ELNK ACTIVE (or INACTIVE) "Hostname"

A Default Route is added using the commands

=>NEW ROUTE 0.0.0.0 "IP Addr of Router"

=>PRT ROUTE

=>ENL ROUTE "Route ID from list"

In LD 137 there are commands to enable & Disable the ELAN as well as seeing its status

ENL ELNK / DIS ELNK / STAT ELNK

ELAN Config – SA & HA LD 117

```
>LD117
 NEW HOST "HOSTNAME"  "IP ADDRESS"
=> new host csact 10.10.10.11
INET Data Added
=> new host csinact 10.10.10.13
INET Data Added

Two Hosts are created for a Dual CPU system

=> chg elnk active csact          Enables Active
=> chg elnk inactive csinact      Enables Inactive
=> prt host
Call Server
 ID  Hostname       IP Address
 3  LOCAL_PPP_IF    137.135.192.4
 4  REMOTE_PPP_IF   100.1.1.1
 9  CSACT           10.10.10.11
 10  CSINACT        10.10.10.13
```

⇒ Chg mask 255.255.255.0 **Sets Subnet Mask**

```
=> new route 0.0.0.0 10.10.10.1

=>prt route
Call Server
 ID  Network      Gateway
  1  0.0.0.0      10.10.10.1

=> enl route 1
ROUTE: "0.0.0.0" "10.10.10.1" enabled
OK
```

⇒ update dbs

```
>LD 137          To enable/disable ELAN
>DIS ELNK
>ENL ELNK
>STAT ELNK       Status of ELAN
```

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

58

Notes

_____

_____

_____

_____

Add Pseudo TTY Ports LD 17

Pseudo TTY ports are used for networked access to the call server. A TTY port is usually associated with a physical serial port whereas PTY's are not.

PTY's are used by the Element Manager and SSH connection to the call server so are essential. The default database has at least one PTY which was there originally to support Telephony Manager. Ensure there are sufficient PTY's to support access.

```
>ld 17
CFN000
MEM AVAIL: (U/P): 29114433   USED U P: 9032899 21241   TOT: 38168573
DISK SPACE NEEDED: 15 KBYTES
DCH          AVAIL:  100  USED:   0  TOT:  100
AML          AVAIL:   16  USED:   0  TOT:   16

REQ  chg                          - Change
TYPE adan                         - Action Device and Number
ADAN new tty 10                   - New TTY on 10
CTYP pty                          - TTY type is a Psuedo TTY i.e. Not connected to a physical port
PORT
DNUM 10
DES  Psuedo tty                   - Description
FLOW
USER mtc sch bug                  - Allow Maintenance, SCH codes and Bug message to be displayed
TTYLOG
BANR

MEM AVAIL: (U/P): 29114341   USED U P: 9032951 21281   TOT: 38168573
DISK SPACE NEEDED: 15 KBYTES
DCH          AVAIL:  100  USED:   0  TOT:  100
AML          AVAIL:   16  USED:   0  TOT:   16

ADAN DATA SAVED
```

Amlex Copyright www.Amlex.Co.UK Personal use only Not for distribution

59

Notes

_____

_____

_____

_____

Removing Loops in CLI LD 17

Because of the use of the default database in our example we have XCT conference circuits provisioned on loops 0 and 16.

The dialogue shows their removal using overlay 17.

```
OVL000
>ld 17
CFN000
MEM AVAIL: (U/P): 29079111    USED U P: 9066128 23334    TOT: 38168573
DISK SPACE NEEDED: 19 KBYTES
DCH              AVAIL:  100   USED:    0   TOT:  100
AML              AVAIL:   16   USED:    0   TOT:   16
REQ  chg
TYPE cequ
DDCS
XCT  x0
 TDS 0  MFS 0  CONF 1
XCT  x16
 TDS 16  MFS 16  CONF 17
XCT
MGTDS
.
.
.
SYNM

MEM AVAIL: (U/P): 29080049    USED U P: 9065251 23273    TOT: 38168573
DISK SPACE NEEDED: 19 KBYTES
DCH              AVAIL:  100   USED:    0   TOT:  100
AML              AVAIL:   16   USED:    0   TOT:   16
REQ
```

Using the "X" prefix in front of the loop number removes it from the configuration

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

60

Notes

_____

_____

_____

_____

Turn on Multi User LD 17

MultiUser allows for more than one connection to be made by a user and is necessary for Element Manager to run correctly.

In addition it allows the use of the !ERR option to check error codes without moving out of an overlay.

```
>ld 17
CFN000
MEM AVAIL: (U/P): 29114249   USED U P: 9033003 21321   TOT: 38168573
DISK SPACE NEEDED: 15 KBYTES
DCH          AVAIL:  100  USED:   0  TOT:  100
AML          AVAIL:   16  USED:   0  TOT:   16
REQ  chg
TYPE ovly
SID
BKGD
FR44
PBXH
TODR
DROL
MID_SCPU
CY45
MULTI_USER on          - Turn on Multi User for the system

MEM AVAIL: (U/P): 29088246   USED U P: 9059006 21321   TOT: 38168573
DISK SPACE NEEDED: 15 KBYTES
DCH          AVAIL:  100  USED:   0  TOT:  100
AML          AVAIL:   16  USED:   0  TOT:   16
```

MULTIUSER allows more a user more than just one connection to the Call Server and must be enabled for EM to work

Amlex Copyright Associates Ltd www.Amlex.Co.uk Personal use only Not for distribution

61

Notes

_____

_____

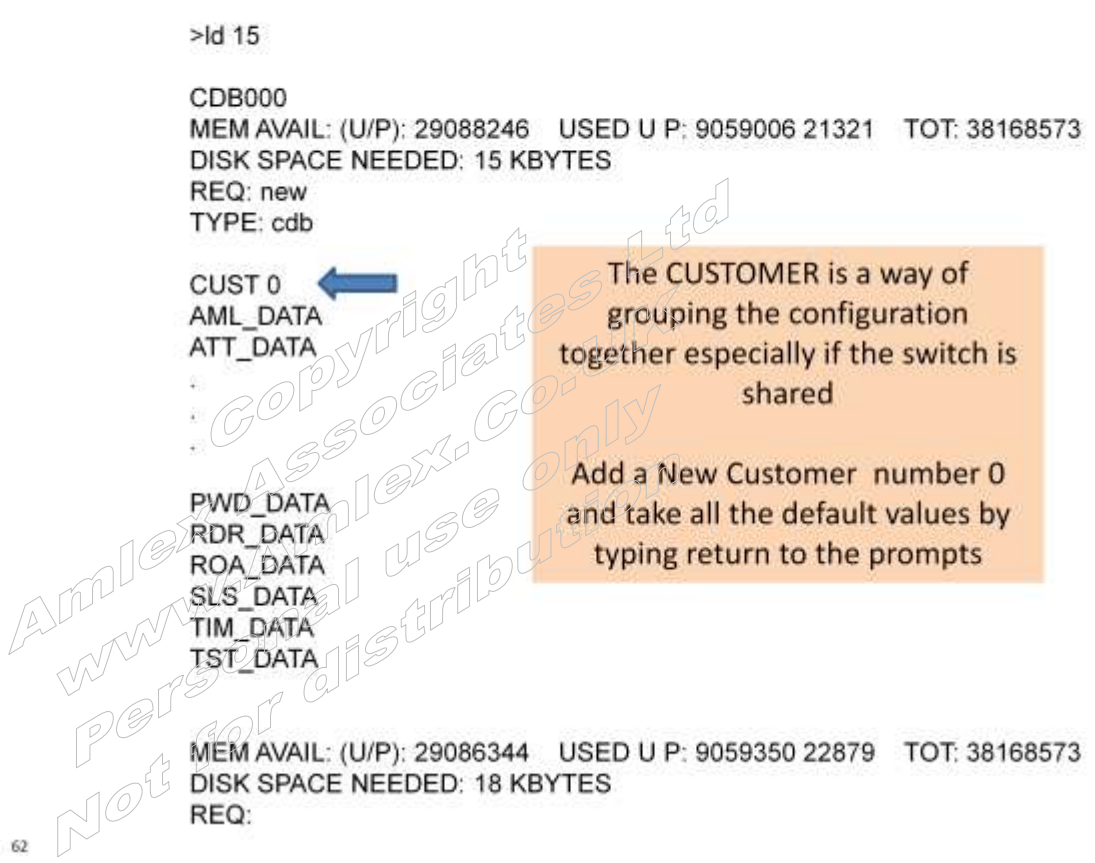
_____

_____

Add a New Customer LD 15

Adding a new customer in LD 15. The Customer is a way of grouping things together when you share a call server.

We must have at least one customer and this will be Customer 0. Without it the system cannot group together the different configuration tables and commands will fail.



62

Notes

_____

_____

_____

_____

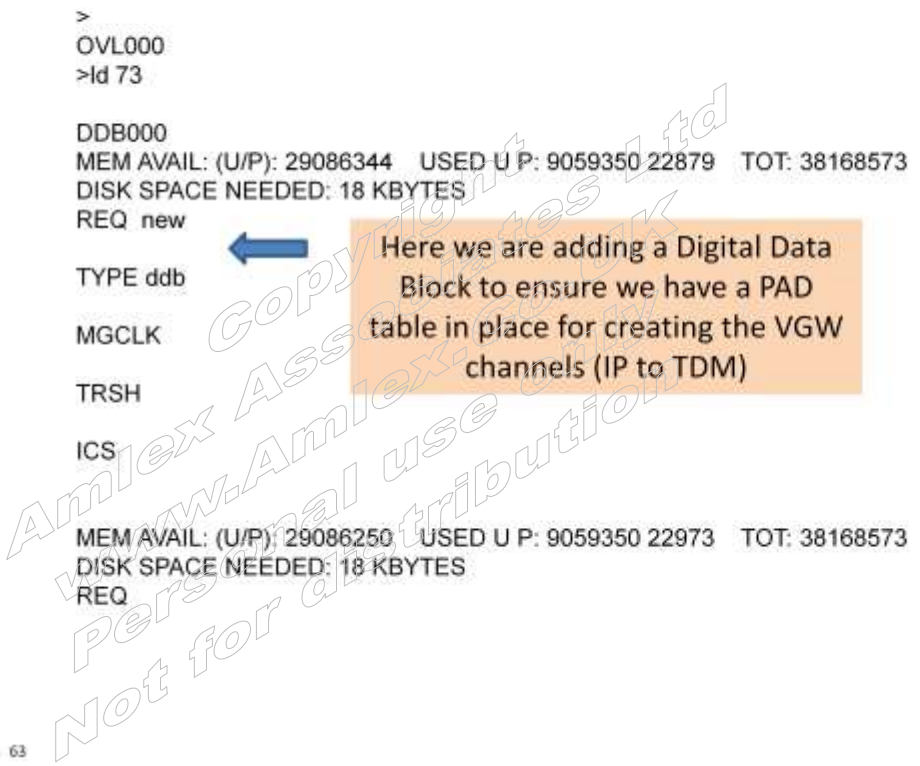
Copyright Amlex Associates Ltd

Add a Digital Data Block LD 73

The Digital Data Block is created so we have a default PAD table which is needed for the Voice Gateway Channels (VGW) used to enable the IP to TDM translation via the DSP & Media cards.

The Digital Data Black is also used when we configure some trunk settings.

These default “Tables” within the database have to be there as the enable the system to link things together as well as setting default values. The configured values may not even be used in our configuration but if the table cant be referenced the system will report a problem.


>
OVL000
>ld 73
DDB000
MEM AVAIL: (U/P): 29086344 USED U P: 9059350 22879 TOT: 38168573
DISK SPACE NEEDED: 18 KBYTES
REQ new
TYPE ddb
MGCLK
TRSH
ICS
MEM AVAIL: (U/P): 29086250 USED U P: 9059350 22973 TOT: 38168573
DISK SPACE NEEDED: 18 KBYTES
REQ
Here we are adding a Digital Data Block to ensure we have a PAD table in place for creating the VGW channels (IP to TDM)
63

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Add Bandwidth Zone LD 117

A Bandwidth Zone is required for configuration of both the IP Phones and the IP Media Gateways.

The simplest way to add a Zone at this point is to create it in LD 117. Using the command “new zone 1”creates a Bandwidth Zone 1 with the default values.

As shown you can allocate actual Bandwidth figures and Strategy but this is much easier done in the Element Manager later on.

Note the PRT INTRA command which prints the zones configured on the system and the values associated. You can see here that Zone 10 is a Virtual Trunk zone thus not available for IP sets .

To add a Zone for the Media Gateways and IP Phones we only need to use the default values as shown below. Later we can edit the values in the Element Manager

```
OVL000
>ld 117
OAM000

=>

=> new zone
Usage: NEW ZONE <zoneNumber> [<intraZoneBandwidth> <intraZoneStrategy> <interZoneBandwidth>
    <interZoneStrategy> <zoneIntent> <zoneResourceType>]

=> new zone 7
Zone 7 added. Total number of zones = 3

=> prt intra
```

Zone	State	Type	Strategy	MO/ BMG/ VTRK	Bandwidth kbps	Usage kbps	Quota kbps	Peak %
1	ENL	SHARED	BQ	MO	1000000	0	0	0
7	ENL	SHARED	BQ	MO	1000000	0	0	0
10	ENL	SHARED	BQ	VTRK	1000000	0	0	0

Number of Zones configured = 3

64

Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Superloops LD 97

A Virtual Superloop can be configured in LD 97 or the Element Manager. The example shows configuring a Superloop 252 as a Virtual Superloop.

Virtual Superloops are required to support the IP sets and Virtual Trunks which will be configured on the system. In reality you may need several Virtual Superloops to support the configuration you require.

```
OVL000
>ld 97

SCSYS000
MEM AVAIL: (U/P): 29086250   USED U P: 9059350 22973   TOT: 38168573
DISK SPACE NEEDED: 18 KBYTES
REQ  chg
TYPE supl
SUPL v252

WRAP UP SUPL 252  (NEW) ..OK

MEM AVAIL: (U/P): 29079111   USED U P: 9066128 23334   TOT: 38168573
DISK SPACE NEEDED: 19 KBYTES
REQ  prt
TYPE supl
SUPL

SUPL  SUPT SLOT XPEC0   XPEC1   SHLF   ZONE0/1  IPR0/1

 252  ---- ---- VIRTUAL -- - -  ---   --- -    ---     ----------
```

Using "V" to prefix the Superloop number changes it into a Virtual Superloop for use with IP Phones and Virtual Trunks

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

65

Notes

_____

_____

_____

_____

The installation of the Linux servers is a three stage process where the Linux Base is installed first. This contains the Common Services which Avaya have added into the Linux core to support the Call Server, Signalling Server, NRS and other processes.

The Base Linux installation also covers the configuration of IP address information as well as the time zone and the Passwords for the two Linux accounts "**root**" and "**admin2**".

Once the Linux Base is installed the initial Security Configuration is done to select the server role, generate the default certificate and add the "**admin**" user password.

Once this is completed the deployment of applications maybe commenced.

6. Linux Base Installation

- Linux Server Installation has three Phases
- Install Linux Base
  - Common services etc
  - Configure
    - IP
    - FQDN – Fully Qualified Domain Name (Hostname + Domain)
    - Timezone
    - Passwords - "root" "admin2" (in rel 6 & 7.0 the "admin2" user account was "nortel")
- Configure Security
  - Certificate
  - "admin" Password
  - Primary Backup or Member
- Deploy Applications

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

66

Notes

_____

_____

_____

_____

The minimum configuration for any Linux server is 2Gb or RAM and a 40Gb Hard disk drive.

Where a CCPM card is being redeployed from an existing release 5 System it will need a RAM upgrade. This is done by adding a second 1Gb memory card into the spare slot. In addition it may need a Hard drive added which needs to be at lease 40Gb capacity but can be larger.

In addition where the CPPM card has been used on a Rel 5 system you will need to ensure that the BIOS is upgraded to Rel 18 or later and that the CMOS has been reset to the Factory Defaults.

All COT's servers are already configured with at least 2Gb of Ram and Hard drives of at least 80Gb.

Minimum Configuration for Linux

- 2 Gb RAM
- 40Gb Hard disk Drive - Upgrades
  - New Cards ship with 250Gb SATA drives
- Supported Devices
  - COTS Servers
  - CPDC
  - CPMG
  - CPPM Card
    - For upgraded Cards – Rel 5 Call server or Sig server
    - 2Gb RAM – 40GB Hard Drive
    - Must Have Upgraded BIOS – 18 or later
    - Must Reset CMOS to Factory Defaults

67

Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

COT's Servers use a DVD installer to load the Linux base software. A separate disk is used to load the Applications software unless centralised deployment is used.

CPPM cards use a Compact Flash card installer. The minimum size for this is 1Gb.

However if a higher capacity card is used the Linux Base software and the Applications Image (.NAI) file can be accommodated. This allows for the loading of the Deployment load from the Compact Flash card. Check the file sizes to ensure you have sufficient capacity as there are now multiple ".NAI " for the basic applications, MAS and Presence.

Installation Media – Linux Servers

- For COTs servers
  - DVD installer
    - Separate disks for Linux and Applications
- For CPPM Cards
  - Minimum 2Gb Compact Flash card for Linux
  - If Using a 4Gb Compact Flash - Linux and Applications may be installed from the same card.
- For CPDC & CPMG Cards
  - Minimum 2Gb USB stick
  - 4Gb USB Stick can have Applications also
- Once the Primary/Deployment server is in place other servers can be installed using NFS across the network.
  - NOTE:- A Boot device (CF/USB) will be required to initiate the process if it is a new installation. **Upgrades** can be performed using NFS without the need for a boot device.

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

68

Notes

_____

_____

_____

_____

CPPM Linux Install

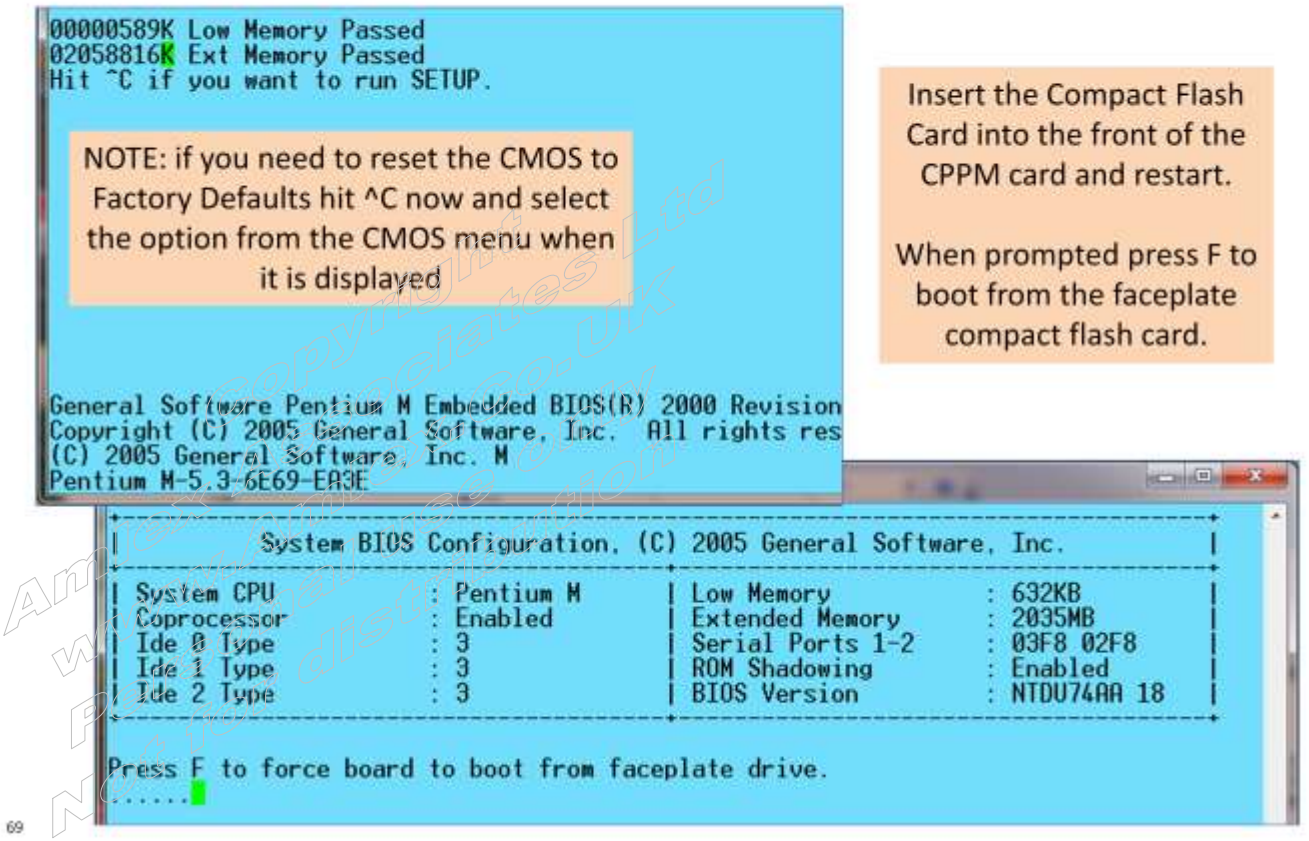
To install the Linux Base :-

1. CPPM - The install Compact Flash card is inserted into the front of the card and the card is restarted. The system will request that an F is pressed to Boot from the installer. (As shown in the diagram)

2. COT's - The DVD is inserted into the drive and the server is restarted. This will force the server to boot to the installer.

3. CPMG/CPDC The USB installer is inserted into the front of the card.

The diagram shows a CPPM card booting with F being pressed to start the installer. Note on the lower picture the EXTENDED MEMORY and the BIOS VERSION. Both of these need to be checked when running Linux.


00000589K Low Memory Passed
02058816K Ext Memory Passed
Hit ^C if you want to run SETUP.
NOTE: if you need to reset the CMOS to Factory Defaults hit ^C now and select the option from the CMOS menu when it is displayed
General Software Pentium M Embedded BIOS(R) 2000 Revision
Copyright (C) 2005 General Software, Inc. All rights res
(C) 2005 General Software, Inc. M
Pentium M-5.3-6E69-EA3E
Insert the Compact Flash Card into the front of the CPPM card and restart.
When prompted press F to boot from the faceplate compact flash card.
System BIOS Configuration, (C) 2005 General Software, Inc.
System CPU : Pentium M
Coprocessor : Enabled
Ide 0 Type : 3
Ide 1 Type : 3
Ide 2 Type : 3
Low Memory : 632KB
Extended Memory : 2035MB
Serial Ports 1-2 : 03F8 02F8
ROM Shadowing : Enabled
BIOS Version : NTDU74AA 18
Press F to force board to boot from faceplate drive.
.....
69

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

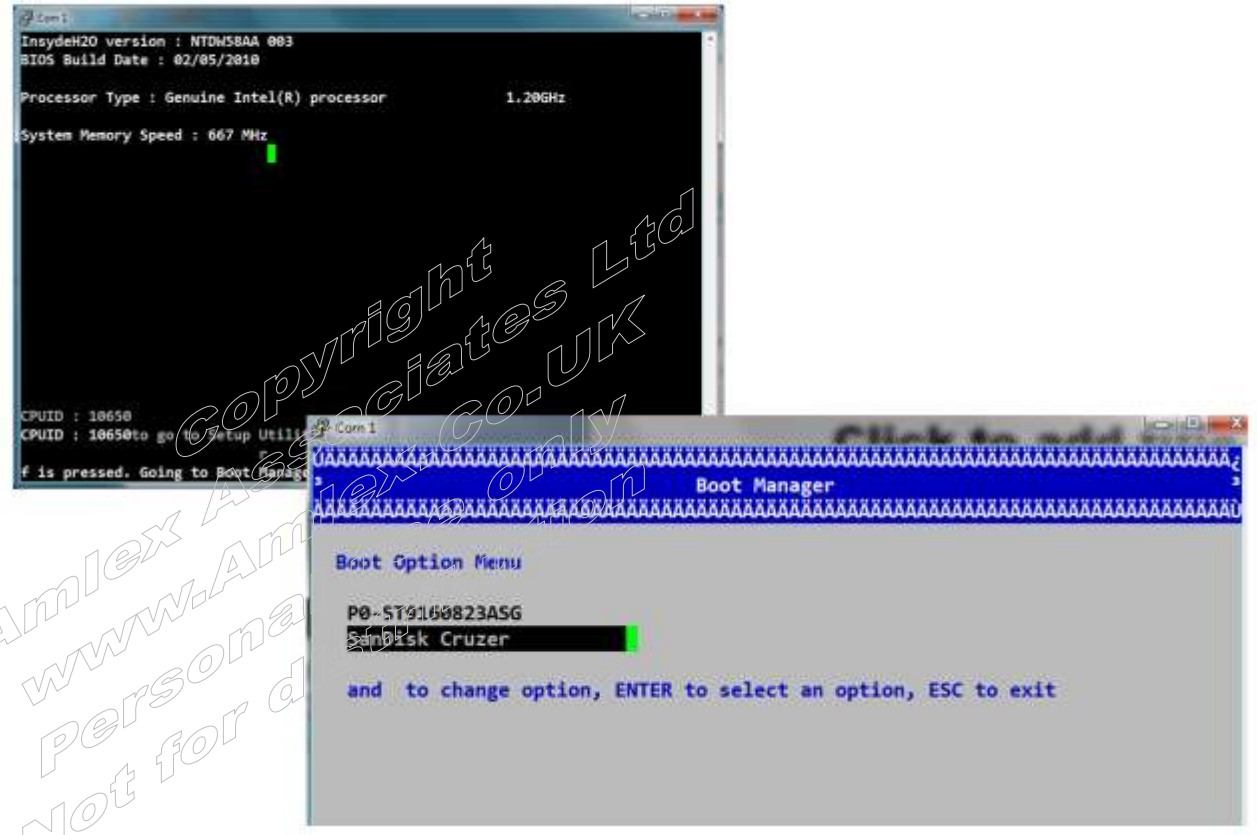
CPMG Linux Install

Here we can see the equivalent boot sequence for the CPMG/CPDC cards.

Again F is pressed to select the Boot Manager (second picture) where the Hard disk or USB stick can be selected.

Use the UP or Down Arrow keys to select the USB installer (Sandisk Cruzer in this example) before hitting the Enter key. The upper option is the hard disk attached to the card.

Note the memory speed on the screen here. On early CPMG cards there were some issues and the advice has been to change the memory speed in the BIOS settings from Auto.


InsydeH2O version : NTDW58AA 003
BIOS Build Date : 02/05/2010
Processor Type : Genuine Intel(R) processor 1.20GHz
System Memory Speed : 667 MHz
CPUID : 10650
Boot Manager
Boot Option Menu
Sandisk Cruzer
and to change option, ENTER to select an option, ESC to exit

Copyright Amlex Associates Ltd www.Amlex.co.UK Personal use only Not for distribution

70

Notes

_____

_____

_____

_____

Starting the Installer

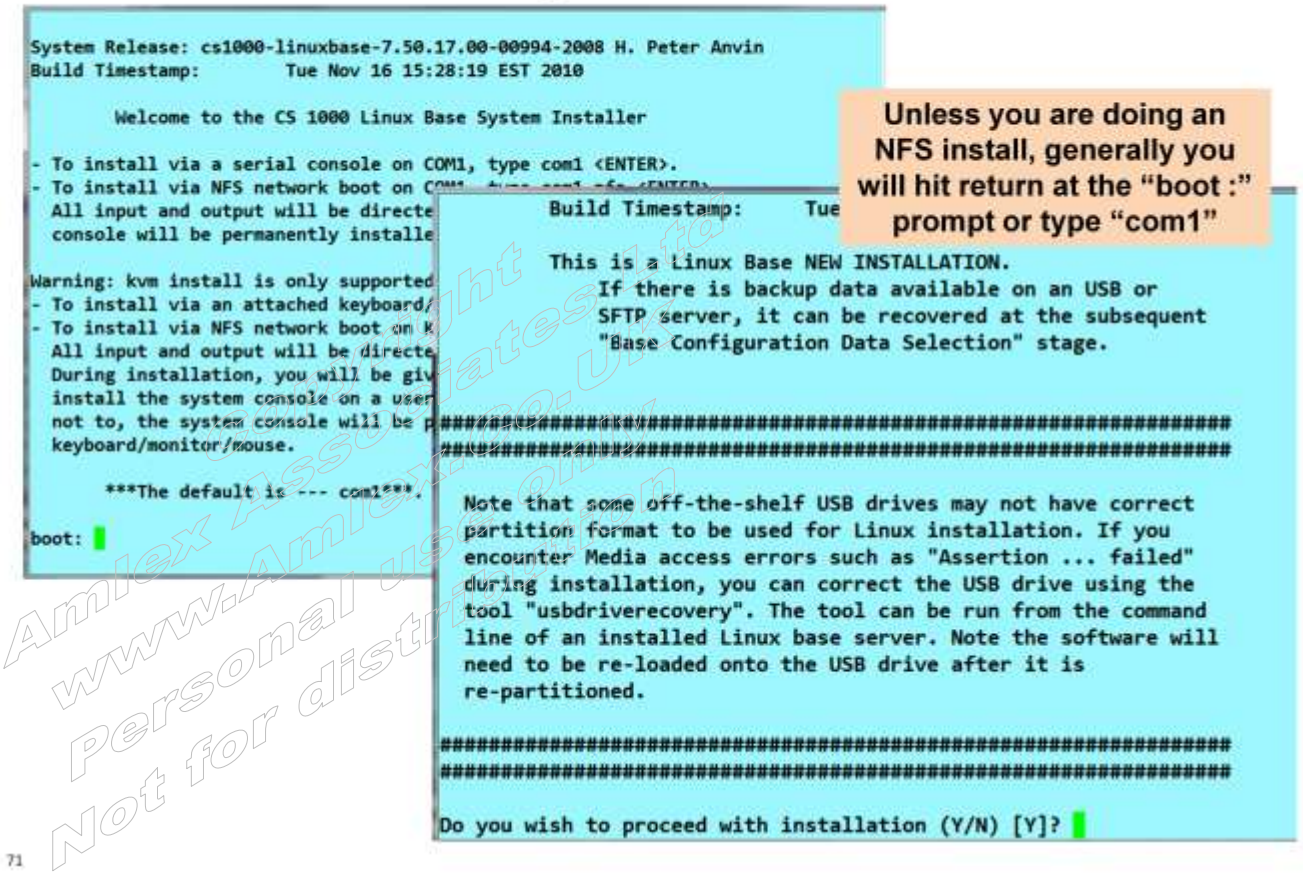
The displays shown are from a CPMG card however the install process is much the same for COT's servers and other cards.

Once the Installer has been invoked the system will load and the upper display will be presented to the user. This will take a few moments.

COM1 is the default option for the installer so one can either type COM1, hit return or just wait and the install will proceed finally loading the Anaconda installer.(Be patient). COM1-NFS is used for NFS installs where both the Linux and Applications are copied from the Deployment Server for installation.

Once the installer has fully started the system will check the hard drive for previous installations. The warning about USB devices is shown on CPMG and CPDC and doesn't necessarily mean there is a problem.

If you select N to stop the installation the system will be halted.


System Release: cs1000-linuxbase-7.50.17.00-00994-2008 H. Peter Anvin
Build Timestamp: Tue Nov 16 15:28:19 EST 2010
Welcome to the CS 1000 Linux Base System Installer
- To install via a serial console on COM1, type com1 <ENTER>.
- To install via NFS network boot on C
All input and output will be directe
console will be permanently installe
Warning: kvm install is only supported
- To install via an attached keyboard/
- To install via NFS network boot on K
All input and output will be directe
During installation, you will be giv
install the system console on a user
not to, the system console will be p
keyboard/monitor/mouse.
The default is --- com1.
boot:
Build Timestamp: Tue
This is a Linux Base NEW INSTALLATION.
If there is backup data available on an USB or
SFTP server, it can be recovered at the subsequent
"Base Configuration Data Selection" stage.
Note that some off-the-shelf USB drives may not have correct
partition format to be used for Linux installation. If you
encounter Media access errors such as "Assertion ... failed"
during installation, you can correct the USB drive using the
tool "usbdriverecovery". The tool can be run from the command
line of an installed Linux base server. Note the software will
need to be re-loaded onto the USB drive after it is
re-partitioned.
Do you wish to proceed with installation (Y/N) [Y]?
Unless you are doing an NFS install, generally you will hit return at the "boot :" prompt or type "com1"

Notes

_____

_____

_____

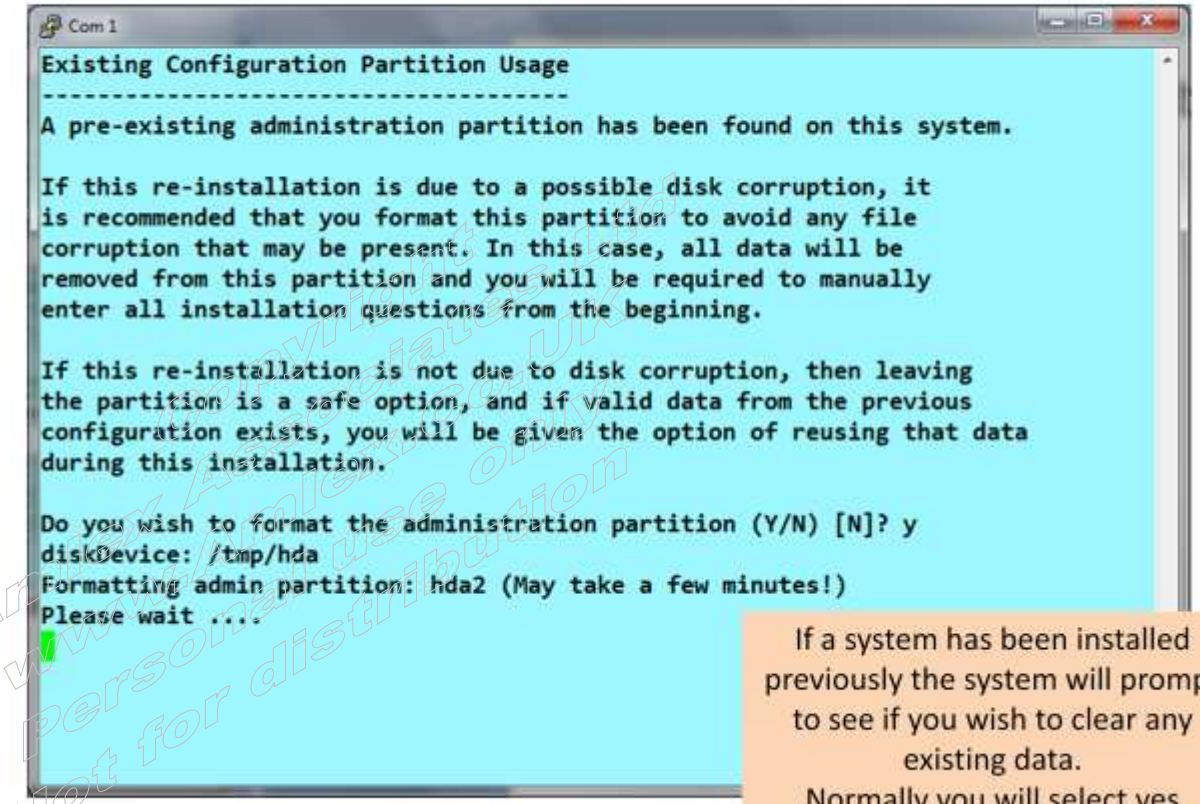
_____

Copyright Amlex Associates Ltd

Format Administration Partition

Where there has been a previous installation the installer programme will prompt you to Format the Administration Partition to clear the original configuration information.

In most cases you will format the partition to ensure the system has no corruption. However if you were performing an upgrade you would likely choose to retain this information.


Com 1
Existing Configuration Partition Usage
A pre-existing administration partition has been found on this system.
If this re-installation is due to a possible disk corruption, it is recommended that you format this partition to avoid any file corruption that may be present. In this case, all data will be removed from this partition and you will be required to manually enter all installation questions from the beginning.
If this re-installation is not due to disk corruption, then leaving the partition is a safe option, and if valid data from the previous configuration exists, you will be given the option of reusing that data during this installation.
Do you wish to format the administration partition (Y/N) [N]? y
diskDevice: /tmp/hda
Formatting admin partition: hda2 (May take a few minutes!)
Please wait ....

If a system has been installed previously the system will prompt to see if you wish to clear any existing data.
Normally you will select yes

Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Base Configuration

The system will then prompt for the type of installation to be carried out. Whether it is to be a new installation, where all of the inputs are made manually or possibly a re-installation where a backup is to be used.

Once this is selected the installer will prompt for the next input.

Backups stored on USB or SFTP can be used to restore a system in he case of a hardware failure or data corruption.

Base Configuration Data Selection
Base configuration data includes:
Network Configuration
Time Zone Configuration
NTP Configuration
DNS Configuration
Local Accounts Passwords
1. Normal installation (do not use any configuration files)
2. Load previously backed up data from USB installation device.
(Note: DO NOT unplug USB installation device at this point.
Upon selection of option 2, further instructions will be shown.
Only one USB storage device should be plugged-in.)
3. Load previously backed up data from SFTP-server.
Select (1-3):1

If you were re-installing you might select option 2 or 3 but for a completely new install select 1 as we have no backup at this point.

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

73

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Network Configuration

The first information requested is the Network configuration for both ELAN and TLAN as well as the Fully Qualified Domain Name (FQDN) to be used.

NOTE:-
The FQDN cannot be changed once it is initially set so ensure you enter it correctly at this stage.

Be aware that the system will prompt for confirmation in case of mistakes so should you enter anything incorrectly you will get the chance to correct it later in the install process.

```
Network Configuration
---------------------
Enter ELAN IP Address: 10.10.10.130
Enter ELAN Netmask: 255.255.255.0
Enter ELAN Gateway IP Address: 10.10.10.1
FQDN (Fully Qualified Domain Name) = Hostname + Domain Name
Enter Hostname: CPMGCoRes
Do you wish to configure a Domain Name (Y/N) [Y]? y
Enter TLAN port Domain Name: CS1K.COM
Enter TLAN IP Address : 10.2.150.130
Enter TLAN Netmask: 255.255.255.0
Enter TLAN Gateway IP Address: 10.2.150.1
Do you wish to configure Tlan with IPv6 Addr (Y/N) [N]?

The Default Gateway will be set to the TLAN Gateway.
Press ENTER to continue.
```

If you make a mistake don't worry as the system will prompt you for any changes you need to make later as you can see here. Note that the IP v6 section is blank as we didn't select it..

Amlex Associates Ltd
www.Amlex.com
Personal use only
Not for distribution

74

Notes

_____

_____

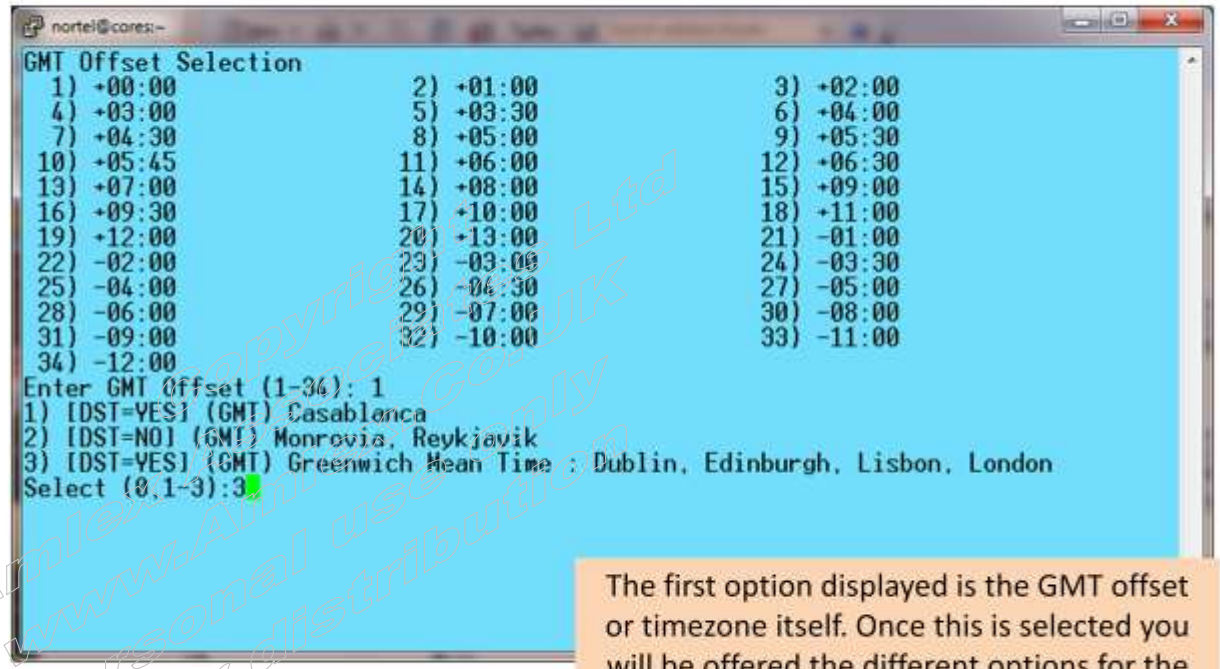
_____

_____

Copyright Amlex Associates Ltd

Timezone & Daylight Saving

The next option is to input the Time zone and Daylight Saving area. This is used in the creation of certificates so should be entered correctly.



The first option displayed is the GMT offset or timezone itself. Once this is selected you will be offered the different options for the Daylight saving times.

Amlex Copyright Amlex Ltd www.Amlex.co.uk Personal use only Not for distribution

75

Notes

_____

_____

_____

_____

Validate Input

Here is shown the first Validation point where you will be given the chance to amend any errors input.

```
Network Configuration Validation
--------------------------------
             ELAN IP Address: 10.10.10.130
     ELAN Gateway IP Address: 10.10.10.1
                ELAN Netmask: 255.255.255.0

                    Hostname: cpmgcores
 Fully Qualified Domain Name: cpmgcores.cs1k.com

            TLAN IP Address : 10.2.150.130
     TLAN Gateway IP Address: 10.2.150.1
                TLAN Netmask: 255.255.255.0

            Enable Tlan IPv6: 0

             Default Gateway: 10.2.150.1

                    Timezone: [DST=YES] (GMT) Greenwich Mean Time : Dublin,
burgh, Lisbon, London

Is this information correct (Y/N) [Y]?
```

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

76

Notes

_____

_____

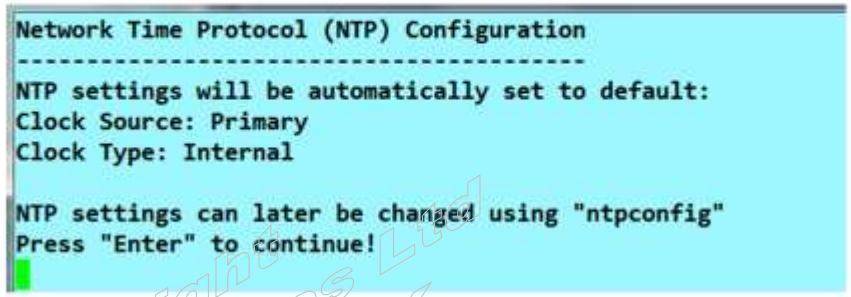
_____

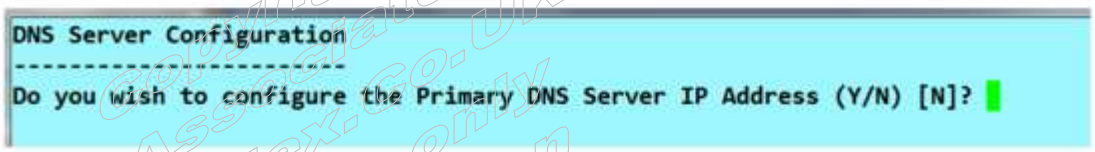
_____

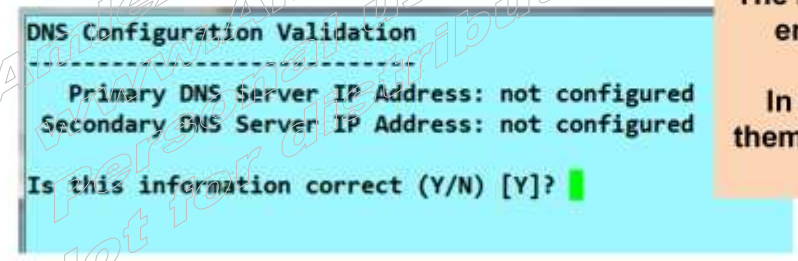
NTP and DNS Configuration

The next options are the NTP server and DNS. The NTP server cannot be set during install. However you can enter a Primary and secondary DNS if you have them.

During the course we will not use a DNS server but will rely upon the Host file on the PC's and Linux servers themselves.


Network Time Protocol (NTP) Configuration
NTP settings will be automatically set to default:
Clock Source: Primary
Clock Type: Internal
NTP settings can later be changed using "ntpconfig"
Press "Enter" to continue!




DNS Configuration Validation
Primary DNS Server IP Address: not configured
Secondary DNS Server IP Address: not configured
Is this information correct (Y/N) [Y]?

The NTP and DNS settings should be entered to ,match the customer network.
In the Labs we will not configure them at install time and will not use a DNS server.

77

Notes

_____

_____

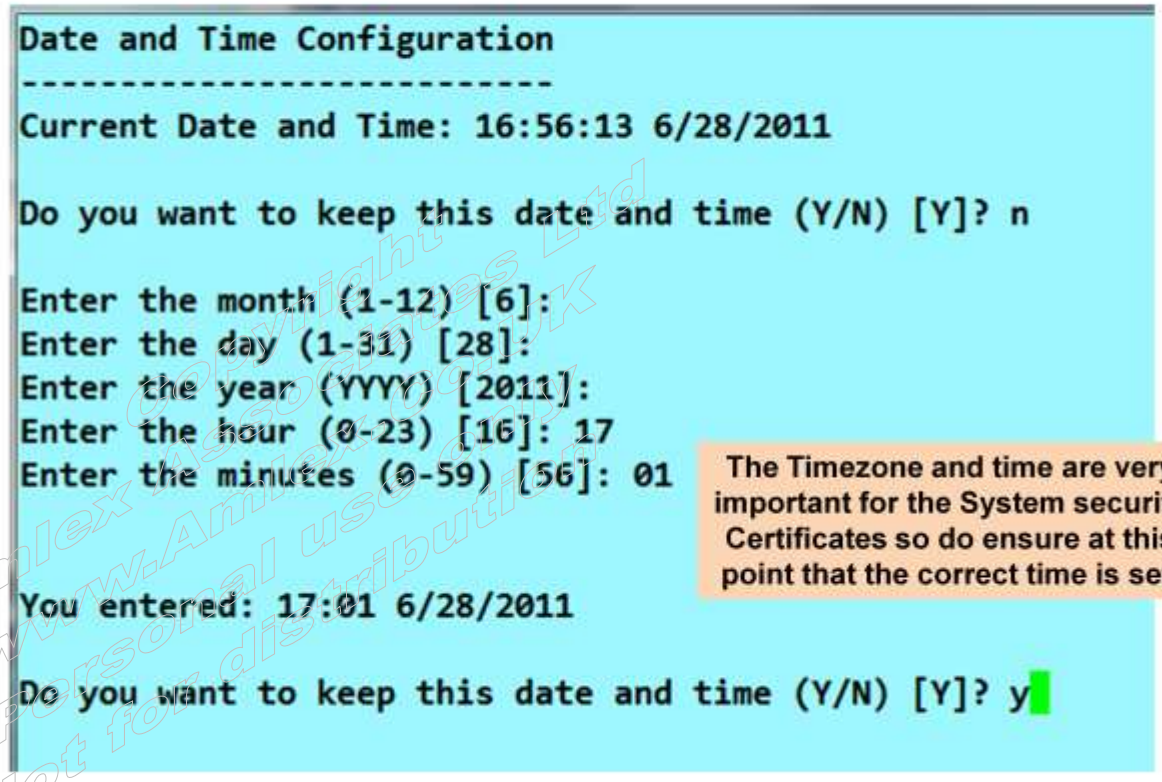
_____

_____

Copyright Amlex Associates Ltd

Setting Server Time

Be sure to check the Date & Time setting of the server you are installing as these will be used when the default certificate is generated. Date errors can cause issues with validity of the certificate so again be careful when setting the date.


Date and Time Configuration
Current Date and Time: 16:56:13 6/28/2011
Do you want to keep this date and time (Y/N) [Y]? n
Enter the month (1-12) [6]:
Enter the day (1-31) [28]:
Enter the year (YYYY) [2011]:
Enter the hour (0-23) [16]: 17
Enter the minutes (0-59) [56]: 01
You entered: 17:01 6/28/2011
Do you want to keep this date and time (Y/N) [Y]? y
The Timezone and time are very important for the System security Certificates so do ensure at this point that the correct time is set.

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

78

Notes

_____

_____

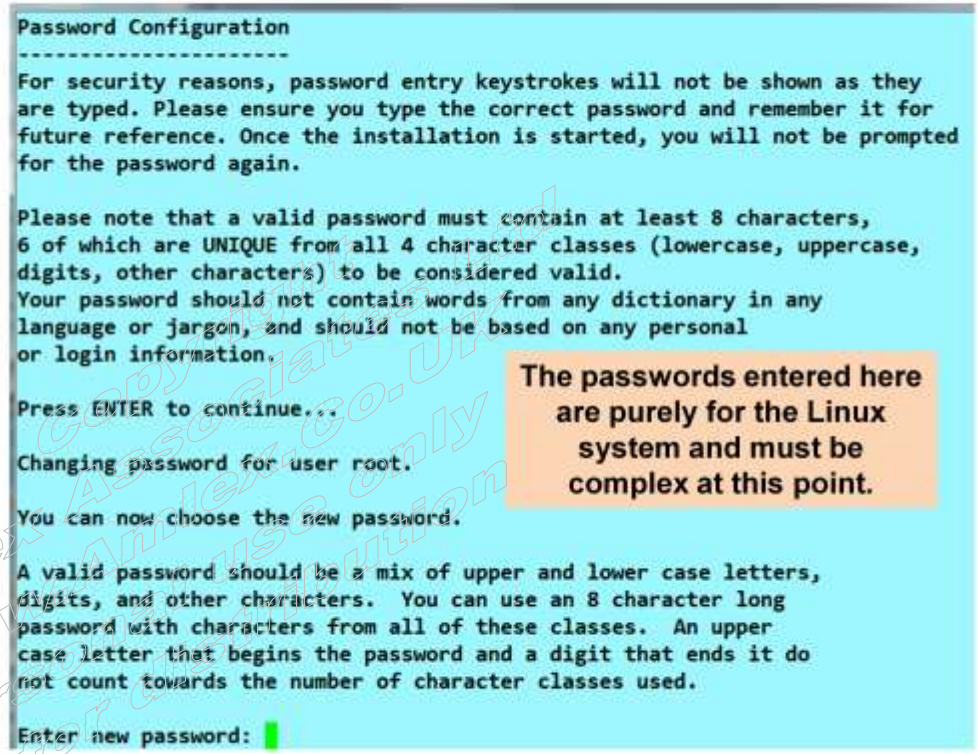
_____

_____

"root" & "admin2" Passwords

Finally the system will prompt you to enter the root & admin2 passwords for the system. It will check that the confirmation is correct before proceeding.

The "admin2" account was formerly the "nortel" account on Release 6.0 & 7.0.


Password Configuration
For security reasons, password entry keystrokes will not be shown as they are typed. Please ensure you type the correct password and remember it for future reference. Once the installation is started, you will not be prompted for the password again.
Please note that a valid password must contain at least 8 characters, 6 of which are UNIQUE from all 4 character classes (lowercase, uppercase, digits, other characters) to be considered valid.
Your password should not contain words from any dictionary in any language or jargon, and should not be based on any personal or login information.
Press ENTER to continue...
Changing password for user root.
You can now choose the new password.
A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.
Enter new password:
The passwords entered here are purely for the Linux system and must be complex at this point.

79

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Deployment Server

The last few questions asked by the system relate to the Passwords to be used on the system and its status as a deployment server.

If the server will be a Deployment Server the installer checks that it is in fact the Primary Security server.

In our example we've answered yes to both of these questions. As release 7 can deploy not only the applications but also the Base Linux itself, the deployment server has to carry a copy of the Linux base for installation on other servers.

```
Deployment Server
-----------------
Do you wish to configure this system as the Deployment Server (Y/N) [N]? y
As a Deployment Server, it must be configured as a Primary Security Server.
Continue configuration as the Deployment Server (Y/N) [N]? y
```

In Rel 7 Linux & Applications can be deployed from Primary Server

```
**************************************************************
*   The final phase to complete the CS 1000 Linux Base System    *
*   pre-installation is now in progress.                         *
**************************************************************
Pre Installation in progress .... (May take a few minutes!)
Please wait ............
```

Be Patient
Installation will start after a few minutes and progress shown on screen

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

80

Notes

_____

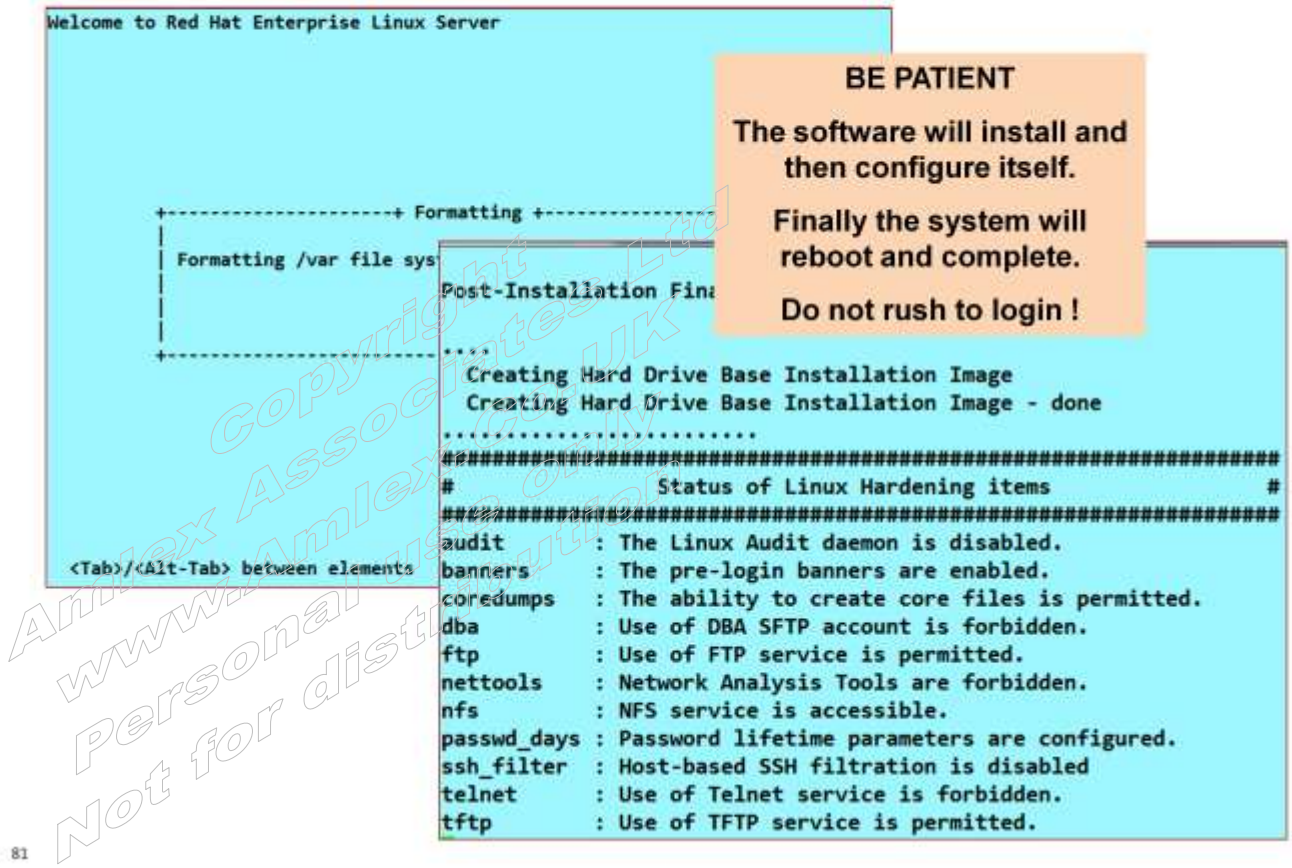
_____

_____

_____

Installation Progress

The System will reboot at the completion of the configuration and in the case of the COT's server it will eject the DVD .


Welcome to Red Hat Enterprise Linux Server
+----------+ Formatting +----------
Formatting /var file sys
<Tab>/<Alt-Tab> between elements
BE PATIENT
The software will install and then configure itself.
Finally the system will reboot and complete.
Do not rush to login !
Post-Installation Fina
Creating Hard Drive Base Installation Image
Creating Hard Drive Base Installation Image - done
Status of Linux Hardening items
audit : The Linux Audit daemon is disabled.
banners : The pre-login banners are enabled.
coredumps : The ability to create core files is permitted.
dba : Use of DBA SFTP account is forbidden.
ftp : Use of FTP service is permitted.
nettools : Network Analysis Tools are forbidden.
nfs : NFS service is accessible.
passwd_days : Password lifetime parameters are configured.
ssh_filter : Host-based SSH filtration is disabled
telnet : Use of Telnet service is forbidden.
tftp : Use of TFTP service is permitted.

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

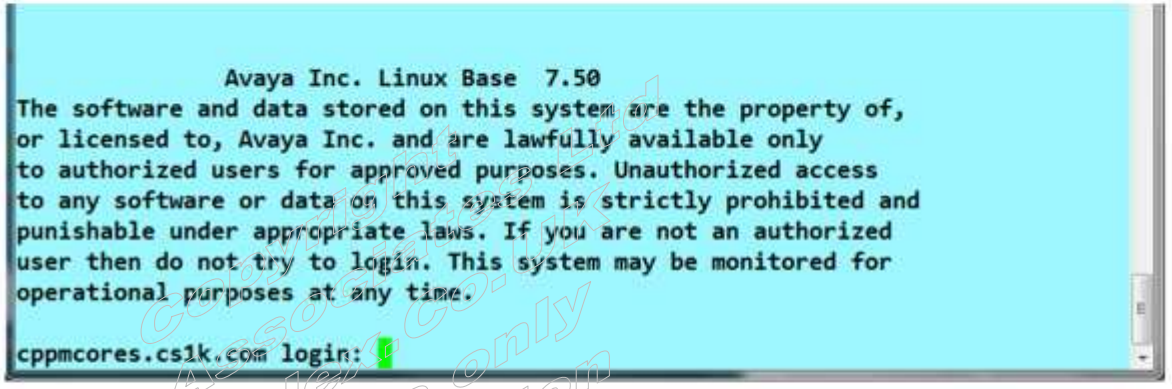
_____

Install Complete Check Logins

The System will reboot at the completion of the configuration and in the case of the COT's server it will eject the DVD .

Once the system completes its reboot, login to both of the Linux accounts, root and admin2 to check they are working correctly before going on to configuring the server security.

If there are any issues at this point they can be rectified now if you can login to the root account. If not you may need to restart the installation.


Avaya Inc. Linux Base 7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.
cppmcores.cs1k.com login:

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Once the installation completes you should be presented with a login banner incorporating the FQDN you specified . Login to check root and admin2 accounts are both working.

82

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

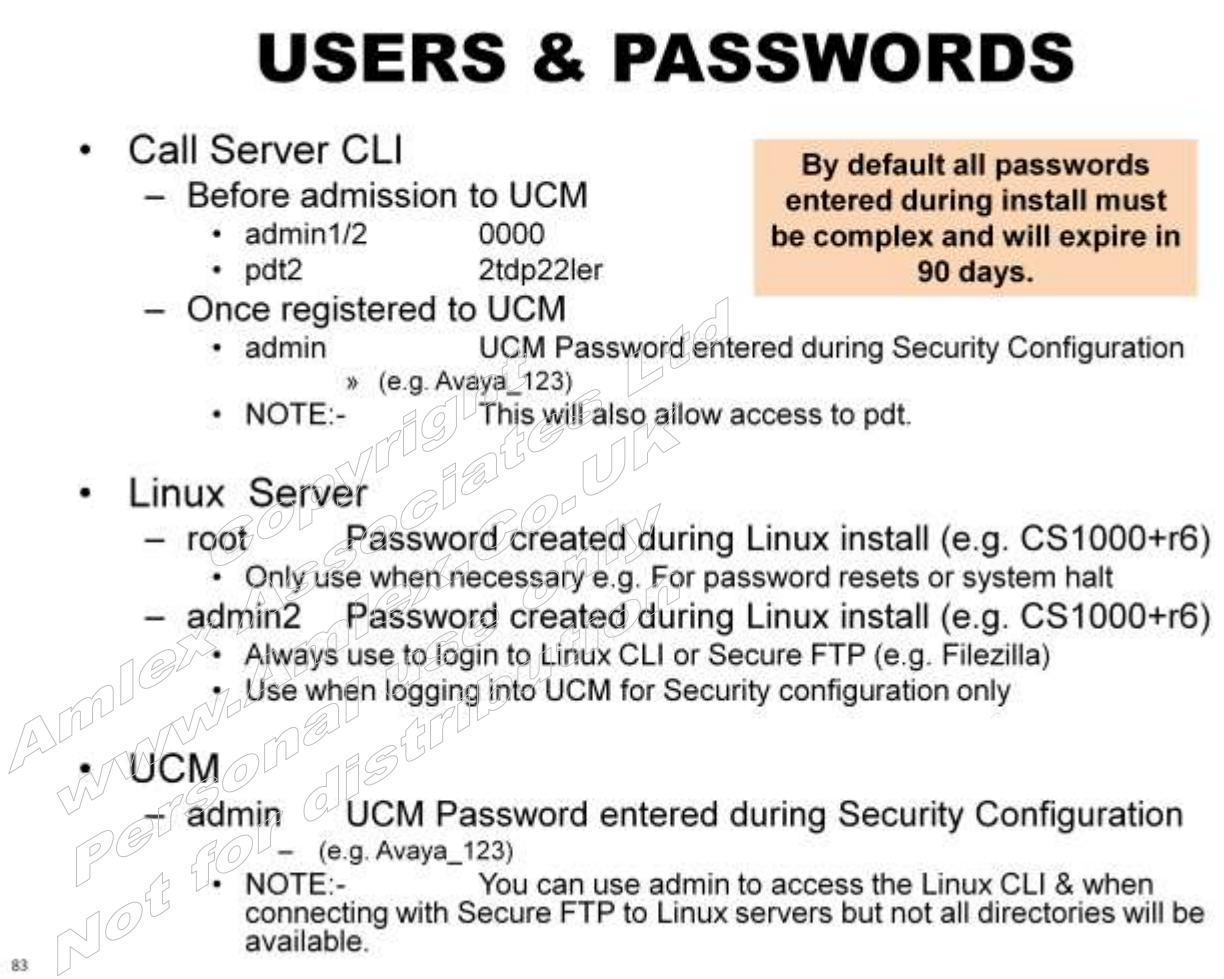
The USERS and PASSWORDS available on the system can cause confusion so it is important to understand which account to use where and when !

In general terms once the system has been configured the rules are :-

1. Use the “admin” account to access the UCM and Call Server command line. Further UCM accounts can be added to allow control of the UCM/Call server access.

2. Use the “admin2” account to login to the Linux Command line or to access the Linux server with SFTP.

3. Use the “root” account only when absolutely necessary e.g. To change a password on the “admin2” account.


USERS & PASSWORDS
Call Server CLI
Before admission to UCM
admin1/2 0000
pdt2 2tdp22ler
Once registered to UCM
admin UCM Password entered during Security Configuration
(e.g. Avaya_123)
NOTE:- This will also allow access to pdt.
By default all passwords entered during install must be complex and will expire in 90 days.
Linux Server
root Password created during Linux install (e.g. CS1000+r6)
Only use when necessary e.g. For password resets or system halt
admin2 Password created during Linux install (e.g. CS1000+r6)
Always use to login to Linux CLI or Secure FTP (e.g. Filezilla)
Use when logging into UCM for Security configuration only
UCM
admin UCM Password entered during Security Configuration
(e.g. Avaya_123)
NOTE:- You can use admin to access the Linux CLI & when connecting with Secure FTP to Linux servers but not all directories will be available.
83

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

The Security Configuration is where you tell the servers which type they will be. You must configure the Primary UCM firstly as every other server relies on it to run correctly.

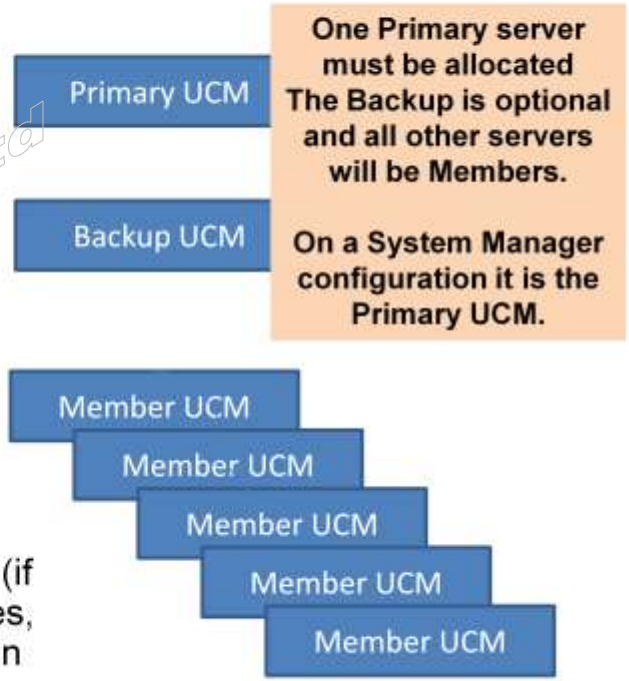
The Primary Server
Is the Deployment server and is the only server which can be used to configure the UCM security. If you are using the Aura System Manager this will be the Primary Security server

The Backup Server
Receives a copy of the Primary's data and can respond to requests made to it by Members when the Primary UCM is offline. The concept of a Backup server is not part of the Aura configuration as the System Manager has its own High Availability options.

The Member server looks to the Primary Server or the Backup if the Primary is offline for all Authentication and Authorisation requests. When using the Aura System Manager all other servers will be Members.

7. Security Configuration

- 3 Types of UCM Server
  - Primary
    - All Configuration
    - Primary Certificate Authority
    - Subscriber Manager
  - Backup
    - Copy of Primary Data
    - Copies of Certificates
    - Handles requests when Primary not available
  - Member
    - Refers to Primary or Backup (if Primary offline) for Certificates, Authentication & Authorisation


Primary UCM
Backup UCM
One Primary server must be allocated
The Backup is optional and all other servers will be Members.
On a System Manager configuration it is the Primary UCM.
Member UCM
Member UCM
Member UCM
Member UCM
Member UCM

Amlex Associates Ltd www.amlex.co.uk Copyright Personal use only Not for distribution

84

Notes

_____

_____

_____

_____

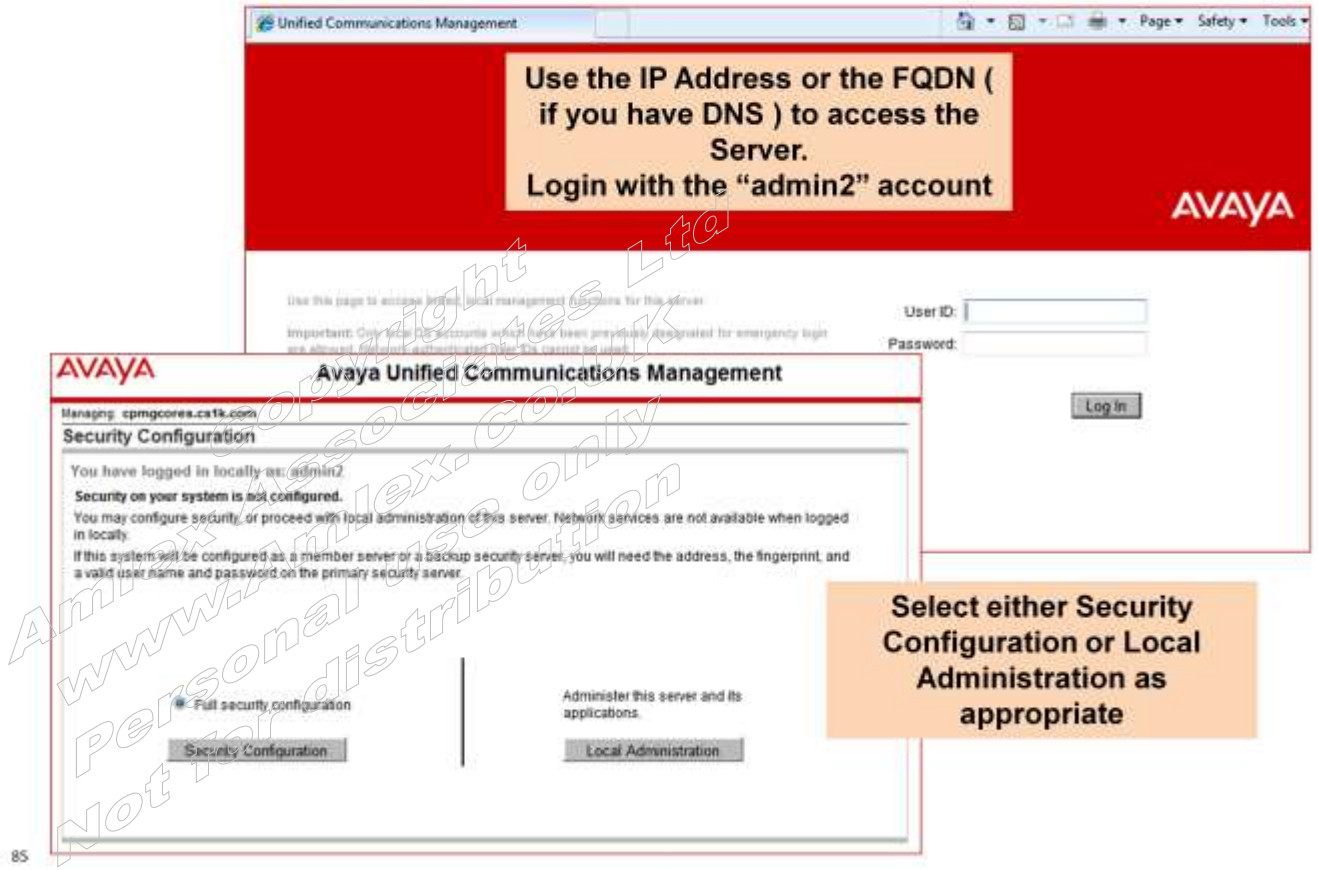
First Login to UCM

To configure the Security information web browse to the server to be configured using either the IP address or the FQDN.

You should get a screen as seen here (top) requesting a user and password.

Login using the “admin2” account and you will be presented with the two options shown here.

If you need to add a local Host entry (i.e. You have no DNS server) click on the Local Administration button shown on the right. Otherwise choose the Security Configuration


Unified Communications Management
Use the IP Address or the FQDN (if you have DNS) to access the Server.
Login with the “admin2” account
AVAYA
User ID:
Password:
Log In
AVAYA
Avaya Unified Communications Management
Security Configuration
You have logged in locally as: admin2
Security on your system is not configured.
You may configure security, or proceed with local administration of this server. Network services are not available when logged in locally.
If this system will be configured as a member server or a backup security server, you will need the address, the fingerprint, and a valid user name and password on the primary security server.
Full security configuration
Security Configuration
Administer this server and its applications
Local Administration
Select either Security Configuration or Local Administration as appropriate

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

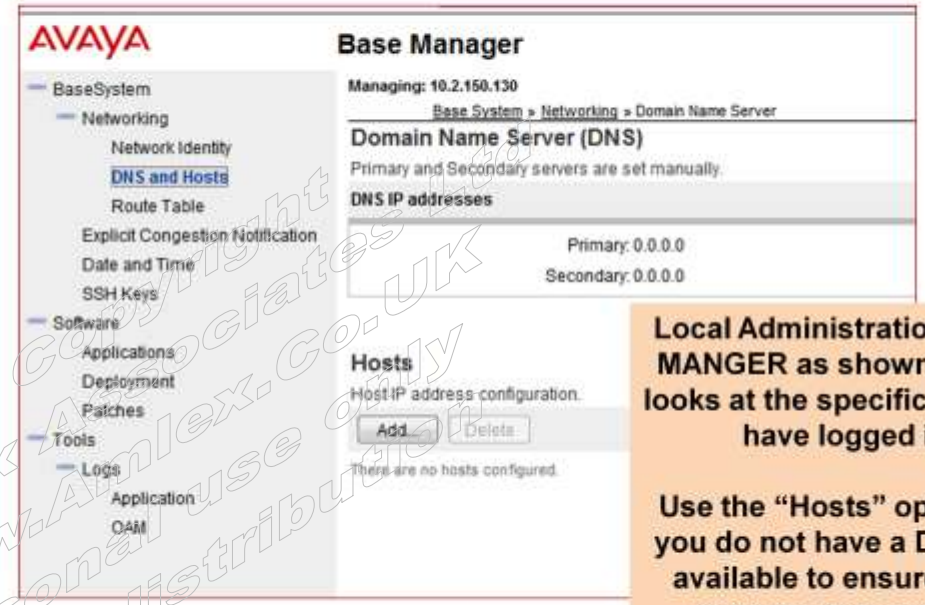
_____

Local Administration

Local Administration allows you to configure some of the elements covered in the initial installation such as the DNS servers.

In addition you can add Host address entries for the server in the same way you might edit the HOSTS file on your PC.

NOTE:- See appendix for adding a Host entry to a PC system for use when no DNS is available.



Local Administration or BASE MANGER as shown here only looks at the specific server you have logged into.

Use the "Hosts" option when you do not have a DNS server available to ensure that the server can access other servers in the UCM e.g. The backup server.

86

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Security Configuration

Once you have completed any Local Administration you will have to logout and log back in so the Security Configuration can be done.

NOTE:-

The FQDN cannot be changed once it is set.

Managing: cpmgcores.cs1k.com
Security Configuration
Security Configuration
Step 1: FQDN validation
Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.
Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): cpmgcores.cs1k.com
N.B. As it states below you cannot change the FQDN once it had been set so be careful during this process. In the event of a failure to create the Default Certificate you will need to re-install Linux.
Note: You can not change the FQDN of a primary or backup server once it has been set.
* Required value.
Next
Cancel

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

87

Notes

_____

_____

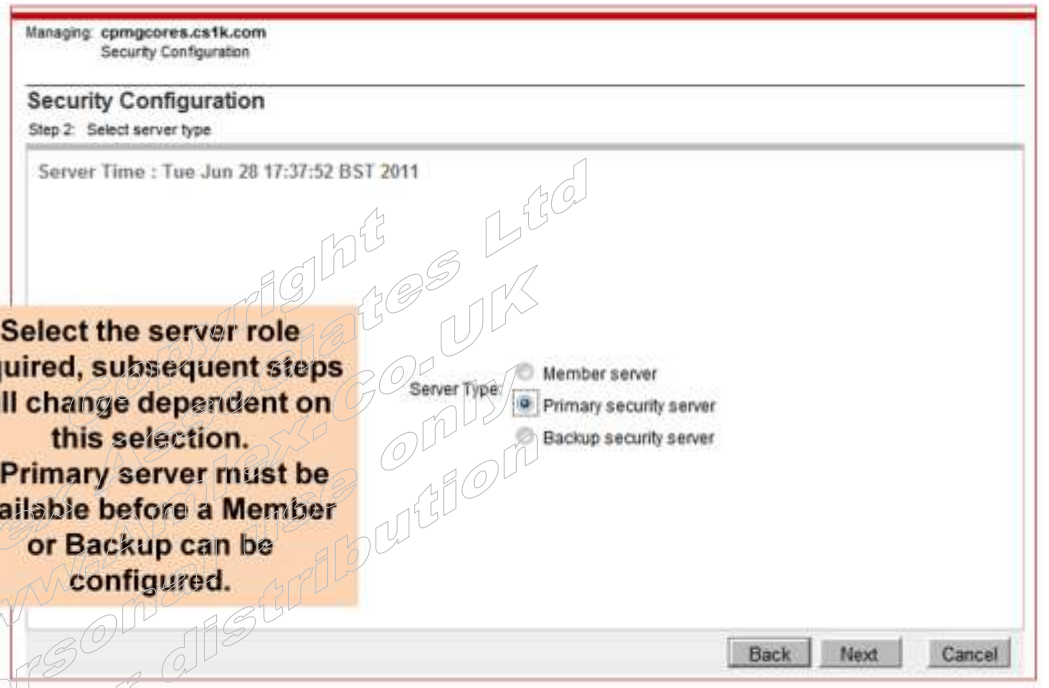
_____

_____

Select Server Role

On this screen you will select the server type to be configured.

You must configure the Primary Security Server before any other server. This is because both the Backup and the Member servers require the Private Certificate Authority of the Primary UCM to generate their own certificates.



Select the server role required, subsequent steps will change dependent on this selection.
A Primary server must be available before a Member or Backup can be configured.

Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

88

Notes

_____

_____

_____

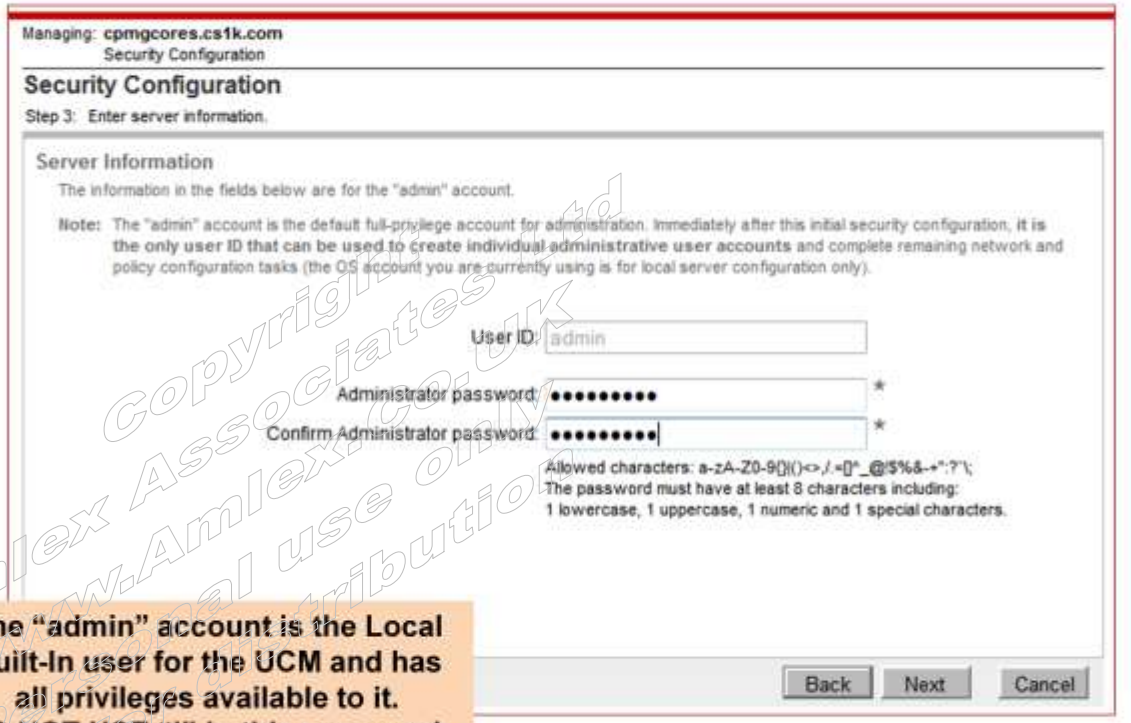
_____

Copyright Amlex Associates Ltd

Admin Password

Here the system is prompting you for the password for the built in “admin” account. This is a UCM account not strictly a Linux account and will be used to access the UCM rather than the Linux CLI.

NOTE:-
All passwords will need to be complex by default . Beware you should not use the “!” in a password as it can be misinterpreted by the system when using the Call Server overlays.


Managing: cpmgcores.cs1k.com
Security Configuration
Security Configuration
Step 3: Enter server information.
Server Information
The information in the fields below are for the "admin" account.
Note: The "admin" account is the default full-privilege account for administration. Immediately after this initial security configuration, it is the only user ID that can be used to create individual administrative user accounts and complete remaining network and policy configuration tasks (the OS account you are currently using is for local server configuration only).
User ID: admin
Administrator password:
Confirm Administrator password:
Allowed characters: a-zA-Z0-9{}|()<>,/.=[]^_@!$%&-+":?`\;
The password must have at least 8 characters including:
1 lowercase, 1 uppercase, 1 numeric and 1 special characters.
Back
Next
Cancel

The “admin” account is the Local Built-In user for the UCM and has all privileges available to it.
DO NOT USE “!” in this password.

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

89

Notes

_____

_____

_____

_____

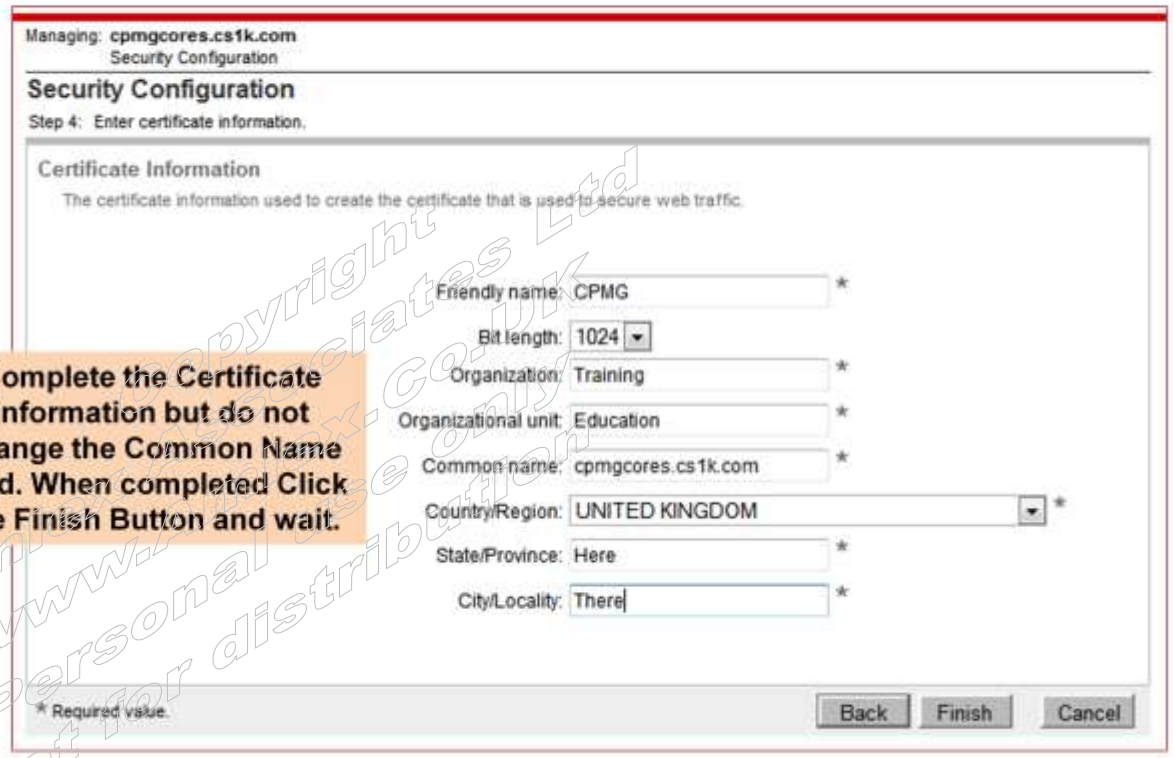
Certificate Configuration

Finally you will be asked for the details of the default certificate that the system is about to create.

DO NOT CHANGE THE COMMON NAME setting at this point.

All other details should be entered to complete the certificate generation. However be careful not to use any special characters when you complete the fields as this can cause the certificate to fail. Even the use of "&" can cause a failed certificate and this will mean you will have to re-install the Linux software.

When you click the FINISH button the certificate will be generated which will take about a minute.



Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

90

Notes

_____

_____

_____

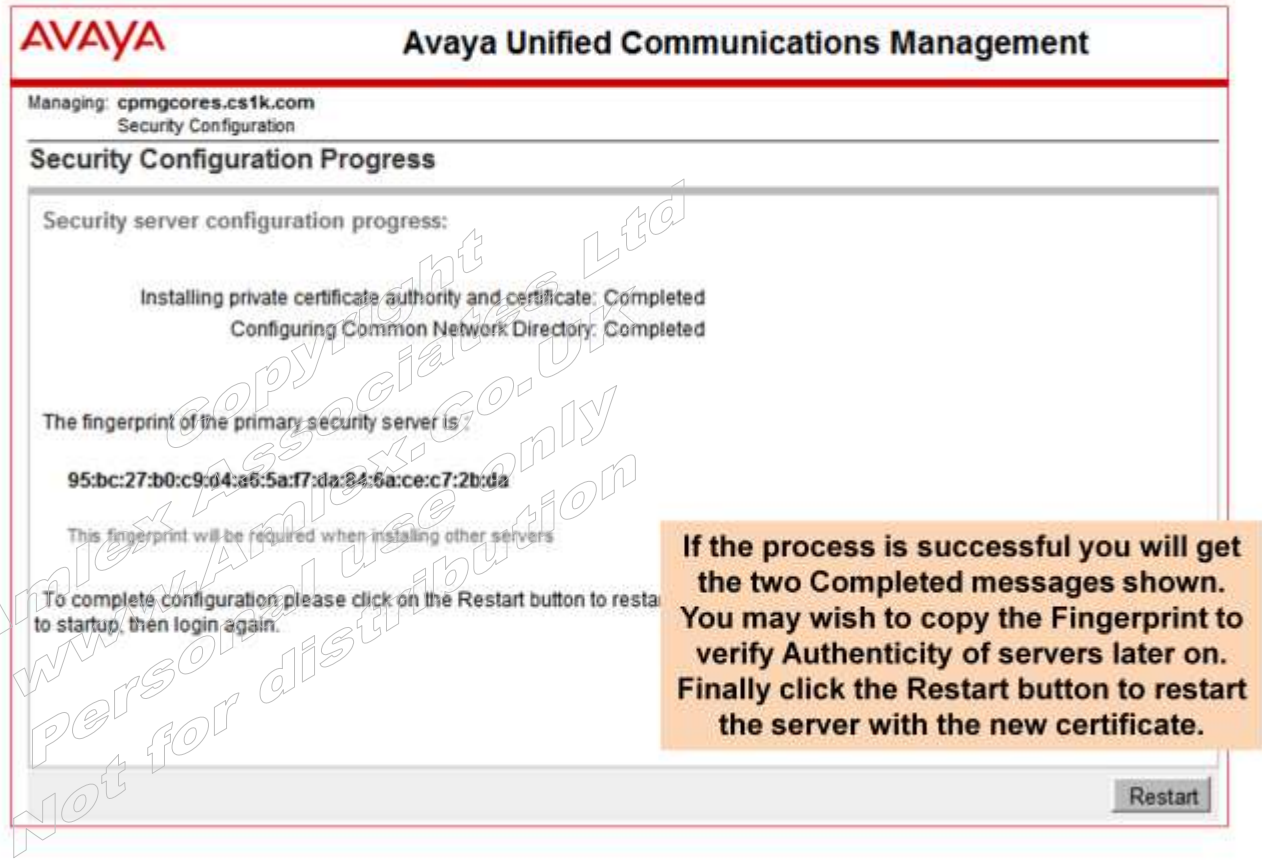
_____

Fingerprint & Restart

If the certificate generation is successful you will be shown the screen here which says the certificate and Common Network Directory are completed.

The Fingerprint is the number the associated with the system and certificate and you may wish to take a copy to compare with server requests when you register the Backup and Member servers.

When you have copied the fingerprint click on the **RESTART** button to restart the UCM software using the new credentials.


AVAYA
Avaya Unified Communications Management
Managing: cpmgcores.cs1k.com
Security Configuration
Security Configuration Progress
Security server configuration progress:
Installing private certificate authority and certificate: Completed
Configuring Common Network Directory: Completed
The fingerprint of the primary security server is:
95:bc:27:b0:c9:04:a6:5a:f7:da:84:6a:ce:c7:2b:da
This fingerprint will be required when installing other servers
To complete configuration please click on the Restart button to resta
to startup, then login again.
Restart
If the process is successful you will get the two Completed messages shown. You may wish to copy the Fingerprint to verify Authenticity of servers later on. Finally click the Restart button to restart the server with the new certificate.

Copyright Amlex Associates Ltd
www.Amlex.co.Uk
Personal use only
Not for distribution

91

Notes

_____

_____

_____

_____

The configuration of Backup and Member servers is much the same as for the Primary server except for the step where the “admin” password is defined.

Instead the system will prompt you for the FQDN of the Primary UCM server. Remember if you are not using a DNS server you will need to have entered a Host entry into each of the different Linux servers via the Local Administration page.

When you have identified the Primary UCM server it will ask for the login details and you should enter the “admin” username and the appropriate password.

You will then be presented with a screen to complete the details for the certificate for the server. Much of this will be pre-populated using the information from the Primary UCM.

Backup & Member Configuration

- The same installation process applies to Member and Backup Servers for the Linux Base
  - Configure IP etc
  - Configure unique FQDN for each server
- Security Configuration
  - Select Server type (Backup or Member)
  - Enter the IP Address of the Primary UCM server
  - Enter the “admin” account details
  - Complete the Certificate information as before
  - Restart when complete and ensure server is added to the ELEMENTS table in UCM.

92

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Web Page Certificate Errors

One problem you will encounter is the Security Certificate error as shown here.

This is because the web browser you are using does not recognise the certificate from the UCM as it is a Private Certificate Authority.

This should be viewed as a warning message and if you are sure you are connecting to the correct server you can continue to the website in question.

To stop the warnings occurring we need to install the Certificate into the Web browser on the management station.

Certificate Error: Navigation Blocked - Windows Internet Explorer
Favorites
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information
The Web Browser is warning you that it does not recognise the Certificate from the server (UCM) you are trying to log onto.
Internet | Protected Mode: On

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

93

Notes

_____

_____

_____

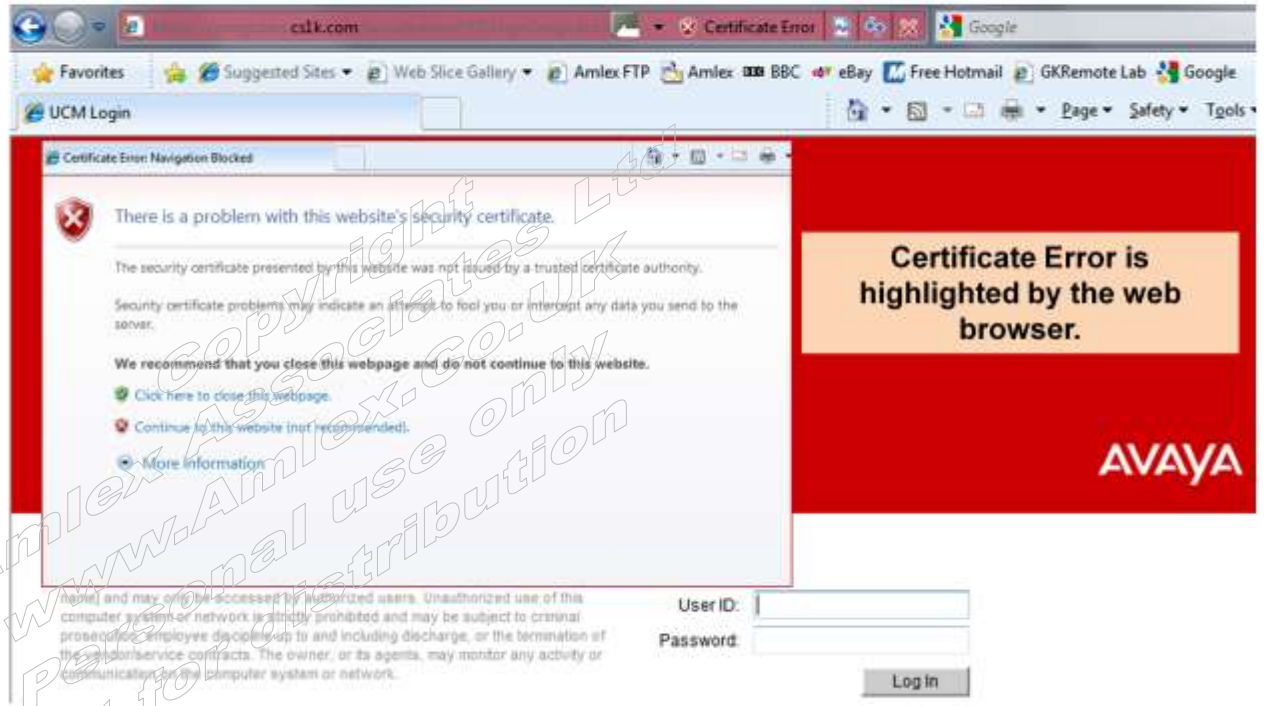
_____

Copyright Amlex Associates Ltd

UCM Login - admin

When we continue to the site we will still see errors in the Address bar on the later versions of Web browser as you can see here.

To stop the problems we need to login as the “admin” user first.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

94

Notes

_____

_____

_____

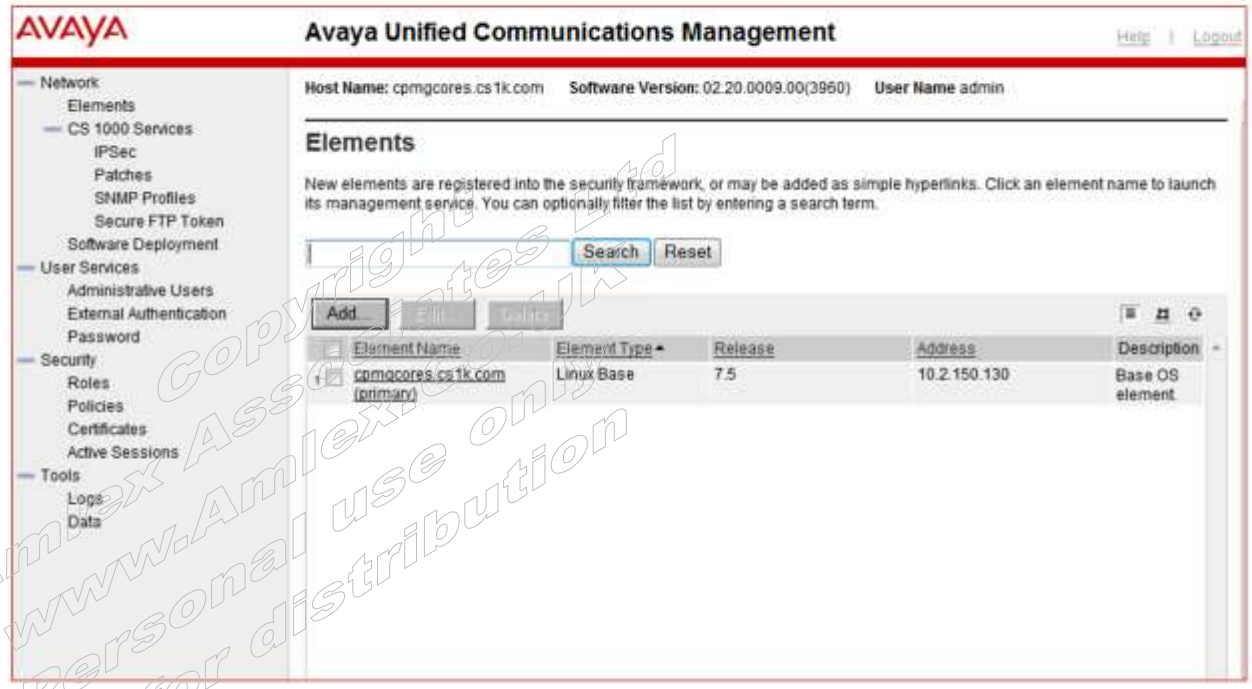
_____

UCM Element List

When you login to the UCM it will present you with the Elements list as shown here. This is a list of all the different elements which make up the UCM security domain and what type they are.

Generally elements are automatically added to the list as they join the UCM domain. However you can manually add Hyperlinks to other systems if required though these will not be part of the Single Sign On domain.

A single server may have several entries in the Elements list to define the different types of software running on the server, e.g. Linux Base, Element Manager NRSM etc.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

95

Notes

_____

_____

_____

_____

Certificate Endpoints

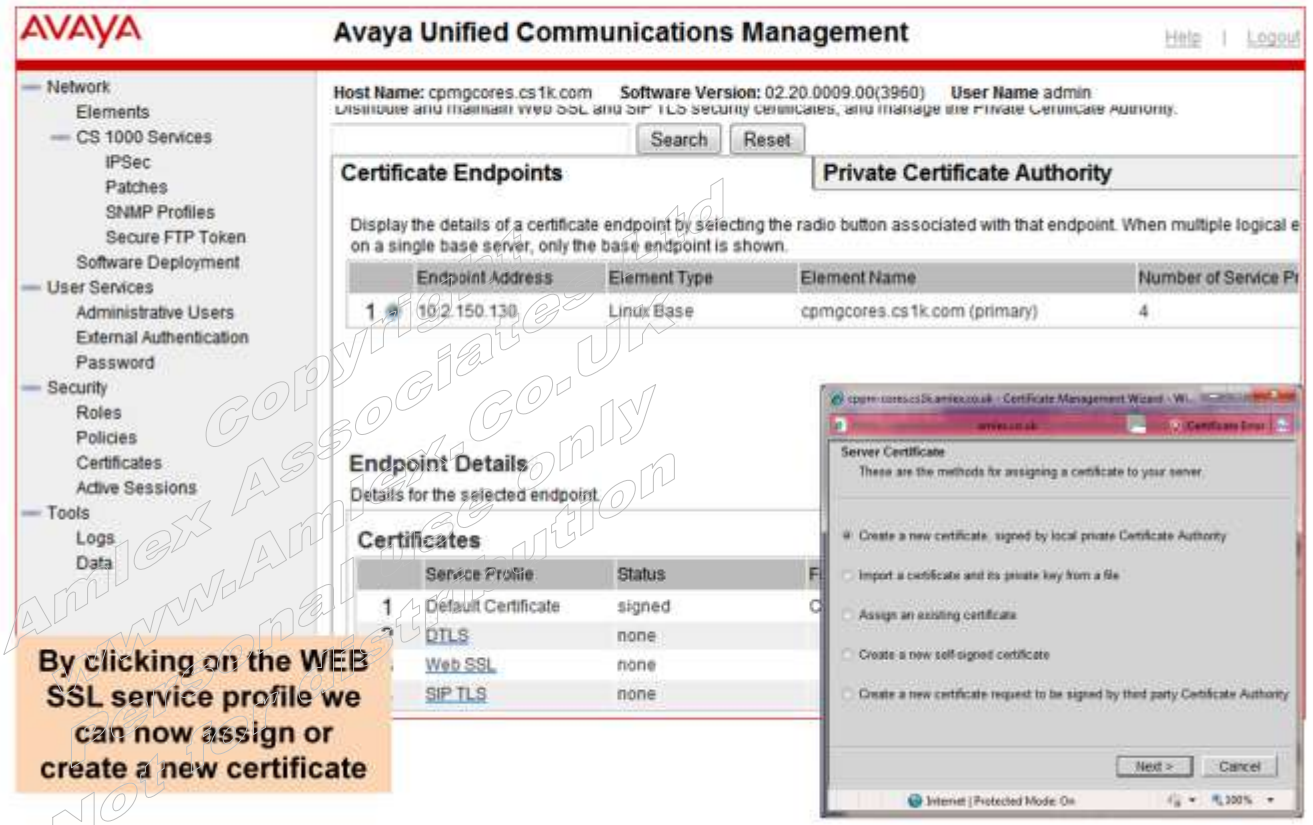
To resolve the issue of the Certificate Error we need to navigate to the **SECURITY/CERTIFICATES** page as shown here.

Notice we are on the Certificate Endpoints tab which shows all of the Endpoints in the UCM domain.

By clicking on the Radio button next to our endpoint it will display the different certificates applicable to this endpoint. In this case we have :-

Default Certificate	UCM
WEB SSL	Web I/F
DTLS	Phones
TLS	SIP

By clicking on the “Web SSL” link we are offered the options of creating or assigning a certificate as none currently exists.



Notes

_____

_____

_____

_____

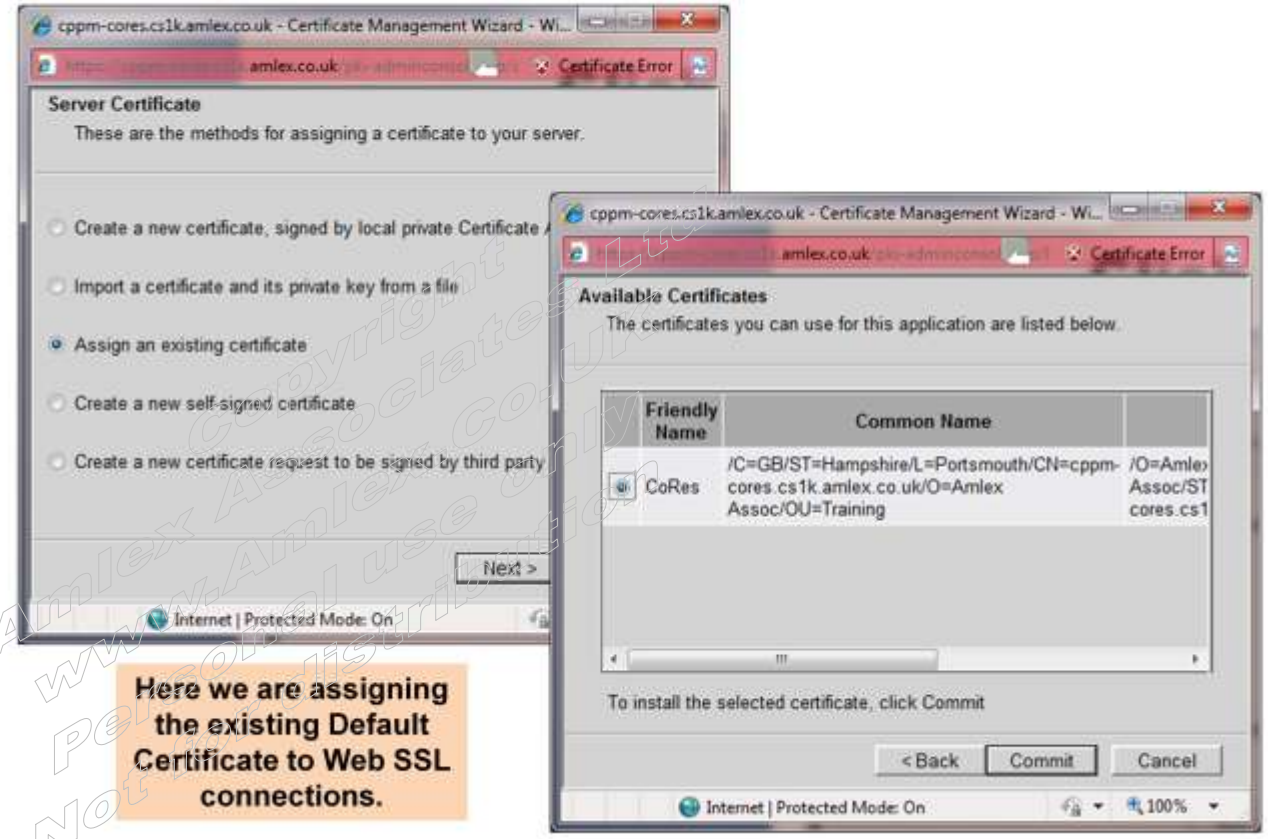
Copyright Amlex Associates Ltd

Assign the Default Certificate

In this instance we are going to assign the existing Default certificate that was created during the initial Security configuration.

The dialogue boxes will walk us through the process of assigning the certificate.

Note the information in the right hand picture which shows the certificate details.


cppm-cores.cs1k.amlex.co.uk - Certificate Management Wizard - Wi...
amlex.co.uk
Certificate Error
Server Certificate
These are the methods for assigning a certificate to your server.
Create a new certificate, signed by local private Certificate A
Import a certificate and its private key from a file
Assign an existing certificate
Create a new self-signed certificate
Create a new certificate request to be signed by third party
Next >
Internet | Protected Mode: On
cppm-cores.cs1k.amlex.co.uk - Certificate Management Wizard - Wi...
amlex.co.uk
Certificate Error
Available Certificates
The certificates you can use for this application are listed below.
Friendly Name
Common Name
CoRes
/C=GB/ST=Hampshire/L=Portsmouth/CN=cppm-cores.cs1k.amlex.co.uk/O=Amlex Assoc/OU=Training
/O=Amlex Assoc/ST
cores.cs1
To install the selected certificate, click Commit
< Back
Commit
Cancel
Internet | Protected Mode: On
100%

Here we are assigning the existing Default Certificate to Web SSL connections.

97

Amlex Associates Ltd Copyright www.Amlex.com Personal use only Not for distribution

Notes

_____

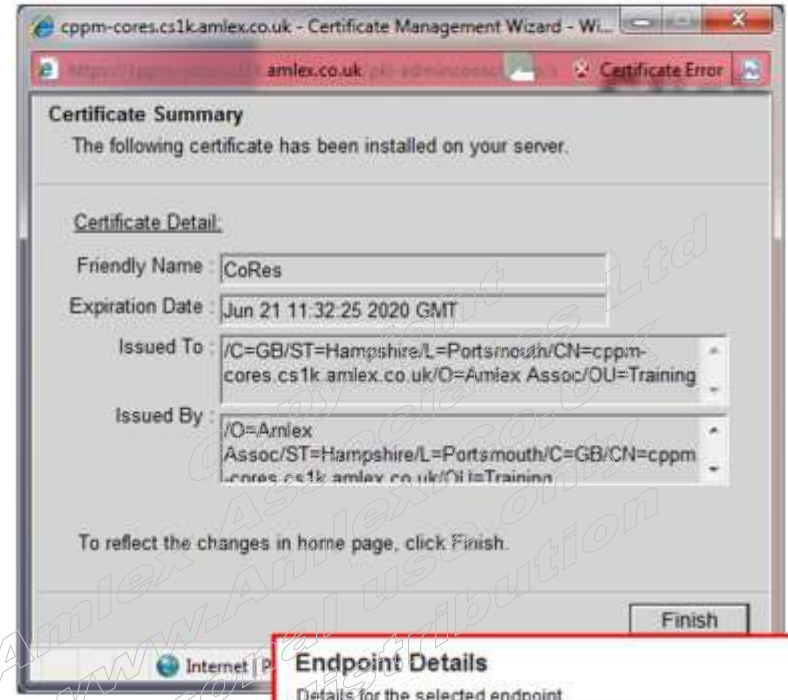
_____

_____

_____

Certificates

Clicking on the Finish button finalises the assignment and you can see in the Lower picture the Web SSL now has the Signed certificate allocated to it.


cppm-cores.cs1k.amlex.co.uk - Certificate Management Wizard - Wi...
amlex.co.uk
Certificate Error
Certificate Summary
The following certificate has been installed on your server.
Certificate Detail:
Friendly Name : CoRes
Expiration Date : Jun 21 11:32:25 2020 GMT
Issued To : /C=GB/ST=Hampshire/L=Portsmouth/CN=cppm-cores.cs1k.amlex.co.uk/O=Amlex Assoc/OU=Training
Issued By : /O=Amlex Assoc/ST=Hampshire/L=Portsmouth/C=GB/CN=cppm-cores.cs1k.amlex.co.uk/OU=Training
To reflect the changes in home page, click Finish.
Finish
Internet

Note the "Signed" status now showing against the WebSSL Profile

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

98

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

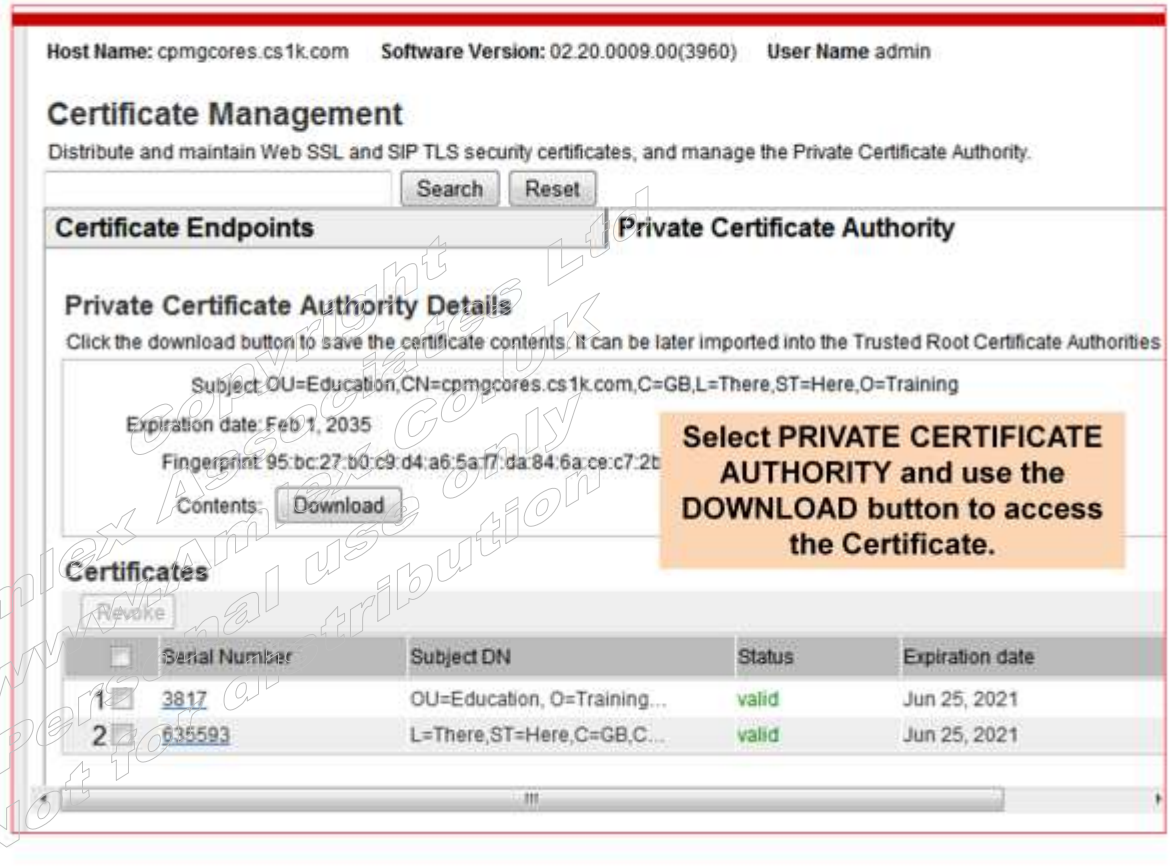
Download Certificate

To add this certificate to our Web Browser we now need to download it and install it into Internet Explorer.

By clicking on the **PRIVATE CERTIFICATE AUTHORITY** tab, we can see the default certificate that was created.

By clicking on the download button this can then be saved to a file, ca.cer (this is the default name and may be changed to match the server it relates to).

Once the file has been saved logout of the browser and shut it down completely.


Host Name: cpmgcores.cs1k.com Software Version: 02.20.0009.00(3960) User Name admin
Certificate Management
Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.
Search
Reset
Certificate Endpoints
Private Certificate Authority
Private Certificate Authority Details
Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities
Subject: OU=Education,CN=cpmgcores.cs1k.com,C=GB,L=There,ST=Here,O=Training
Expiration date: Feb 1, 2035
Fingerprint: 95:bc:27:b0:c9:d4:a6:5a:f7:da:84:6a:ce:c7:2b
Contents: Download
Select PRIVATE CERTIFICATE AUTHORITY and use the DOWNLOAD button to access the Certificate.
Certificates
Revoke
Serial Number
Subject DN
Status
Expiration date
1 3817 OU=Education, O=Training... valid Jun 25, 2021
2 635593 L=There,ST=Here,C=GB,C... valid Jun 25, 2021

99

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

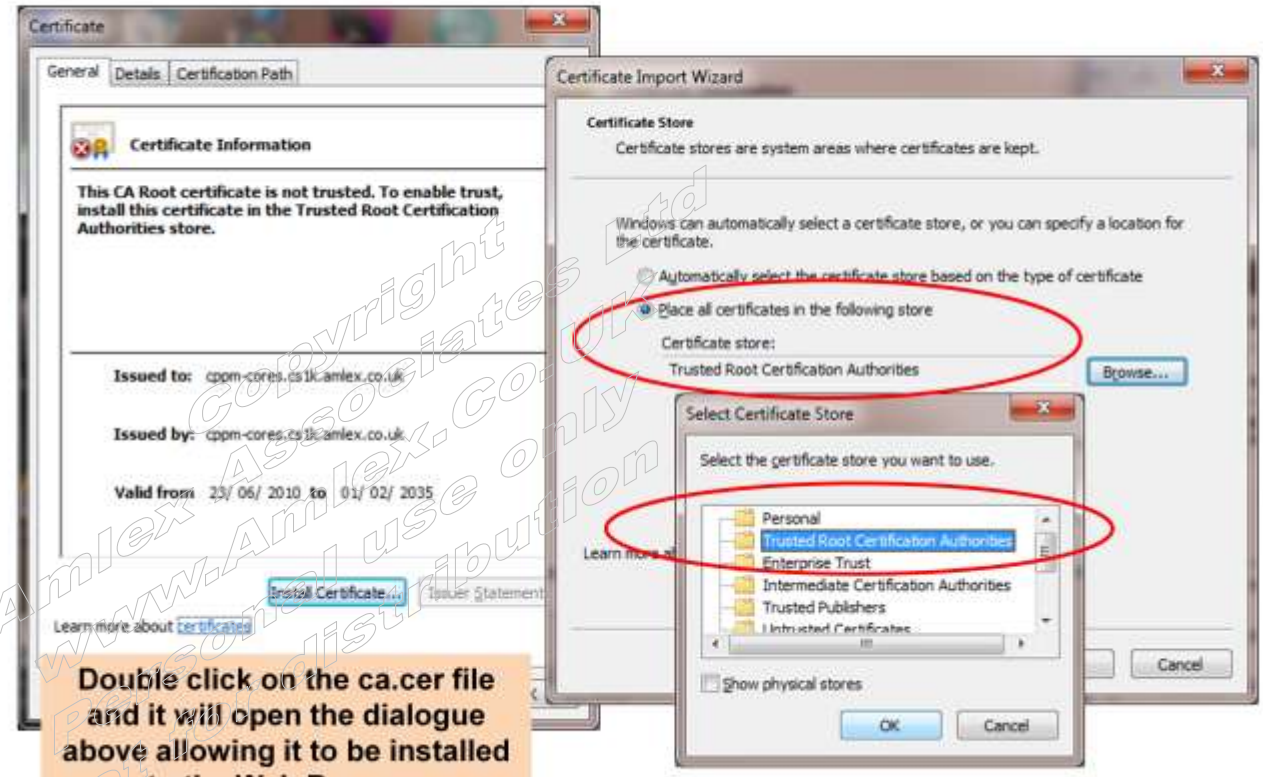
Install Certificate to IE

If you locate the certificate file you downloaded and then double click on it the dialogue shown here will open which can be used to install it to the Web browser.

Make sure that when you click on the install button that you choose the option to **PLACE ALL CERTIFICATES IN THE FOLLOWING STORE** and then select the location shown **TRUSTED ROOT CERTIFICATION AUTHORITIES**.

Once completed reopen the web browser and connect to the UCM using the FQDN (Not the IP address) and you should find that the certificate errors have now stopped.

NOTE:-
You must use the FQDN to access the UCM to avoid the certificate error messages. This is because the system uses the FQDN to resolve the certificate to be used. Using the IP address to access the server will generate the certificate error messages.


Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: cppm-cores.cs1k.amlex.co.uk
Issued by: cppm-cores.cs1k.amlex.co.uk
Valid from 23/ 06/ 2010 to 01/ 02/ 2035
Install Certificate...
Issuer Statement
Learn more about certificates
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Show physical stores
OK
Cancel
Cancel
Double click on the ca.cer file and it will open the dialogue above allowing it to be installed to the Web Browser

100

Notes

_____

_____

_____

_____

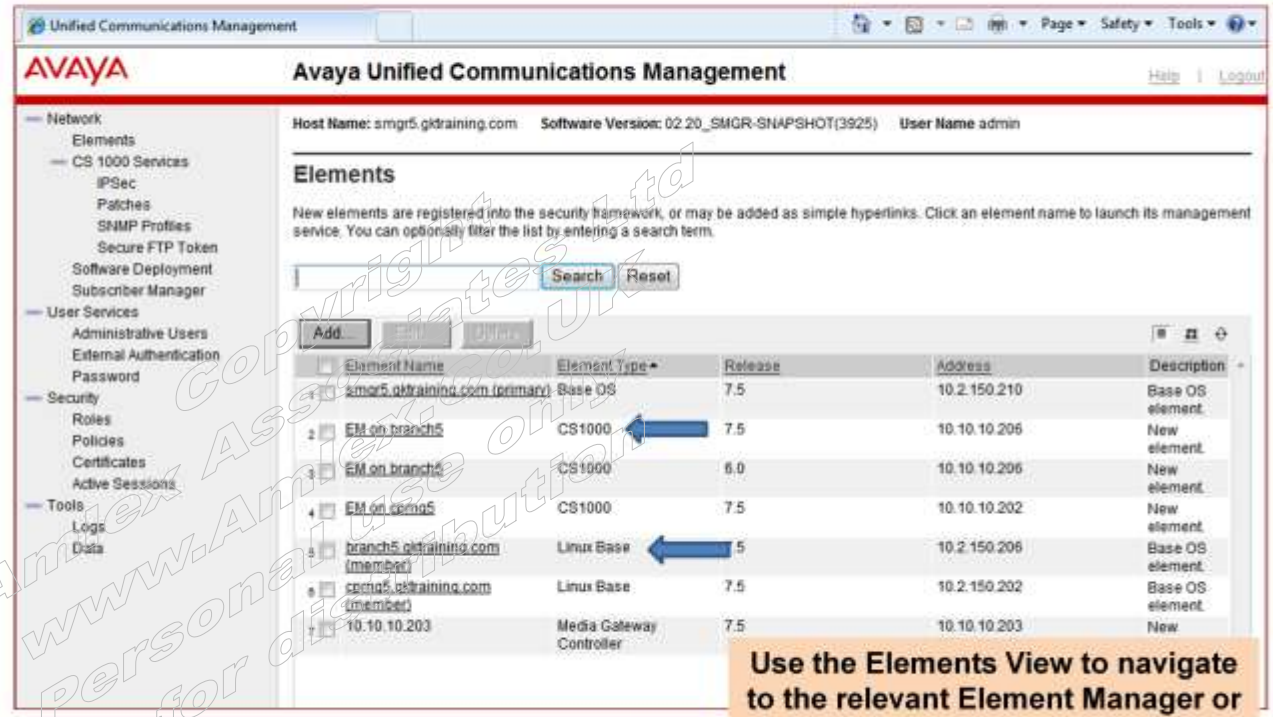
Copyright Amlex Associates Ltd

UCM Element List

When you login to the UCM it will present you with the Elements list as shown here. This is a list of all the different elements which make up the UCM security domain and what type they are.

Generally elements are automatically added to the list as they join the UCM domain. However you can manually add Hyperlinks to other systems if required though these will not be part of the Single Sign On domain.

A single server may have several entries in the Elements list to define the different types of software running on the server, e.g. Linux Base, Element Manager NRSM etc.



Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

101

Notes

_____

_____

_____

_____

The Avaya Linux installed onto the base hardware includes the Common Services. These are the programmes that allow the system to function as part of a CS1000 UCM environment.

Corporate Directory – Allows the creation of a Corporate Directory file for Upload to the CS1000 systems.

IPSec – Controls the encryption of ELAN messages between the CS1000 devices.

Numbering Groups are used by Unicode Directories

Patches – is the Centralised Patching manager for Linux, CoRes Call server and Loadware Patches. It allows them to be uploaded to a central point for distribution.

SNMP Profiles – is used to define SNMP actions and trap destinations.

Secure FTP Token – manages the SFTP token generation and distribution to all the servers. SFTP is used to securely transmit files.

Software Deployment – centralised Application installations to all UCM Linux servers.

Subscriber Manager – an automation link to external Directories.

UCM Common Services

- IPSec
  - Management of Secure ELAN
- Numbering groups
  - Used by Unicode Name Directory
- Patches
  - Central Deployment of Linux patches
  - Deployment of Co-Resident Call Server patches
  - Centralised Loadware management
- SNMP Profiles
  - Setup of SNMP Elements
  - Trap distribution
- Secure FTP Token
  - Manages regeneration of Token used by SFTP
- Software Deployment
  - Centralised Application Deployment
    - CS , SS , EM , NRS etc.
  - UCM Backup & Restore

Copyright Amlex Associates Ltd www.Amlex.Co.Uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

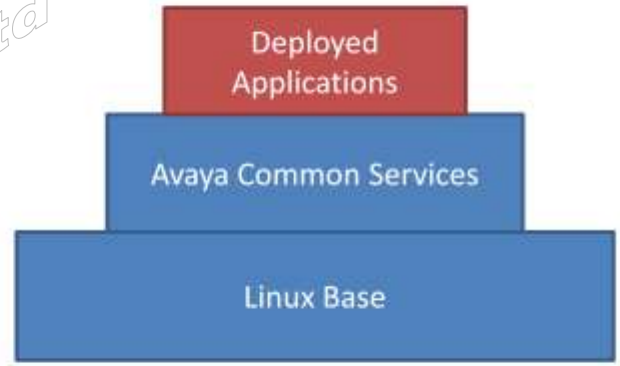
The Software Deployment is the next stage of the installation and as you can see from the diagram the applications are installed over the Linux and Common Services.

The following examples show a Centralised Deployment i.e. From the Primary UCM/Deployment server (in this case to itself) .

Remember however that there is the option, if the Primary UCM is not available to deploy locally using the Base Manager for the server you wish to deploy.

8. Software Deployment

- Linux Base install
  - Creates Linux platform
  - Avaya Common Services
- Deployment
  - Defines Applications to run on different servers
- Options
  - Call Server
  - Signalling Server
  - Element Manager
  - NRSM
  - SIP Line Gateway
  - Subscriber Manager
  - MAS
  - Presence



Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

103

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Software deployment is changed from Release 6 and now features Pre-Deployment of the various servers. This allows configuration work to be carried out before hardware is available.

In addition the Deployment server can now also deploy the Linux Base software for both upgrades and new installations.

Software Deployment

- Pre Deployment
  - Select Applications to be deployed prior to activation
- Deployment of Linux Base to servers
  - Deployment Server can be setup to load Linux to remote servers
  - Centralised Configuration

104

Amlex Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____
_____
_____
_____

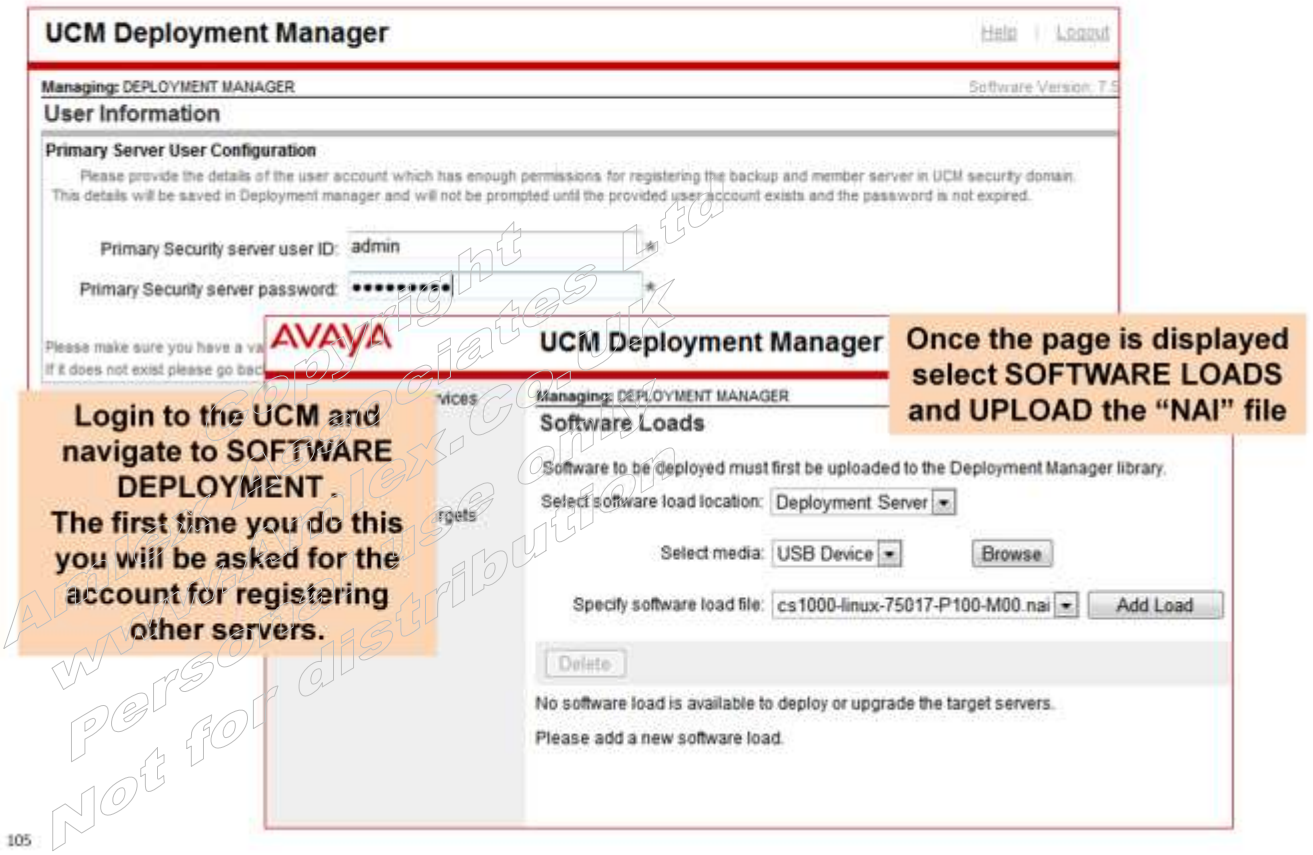
Deployment Software Load

The first task is to add the ".nai" (Application Image) file which contains all the software for the applications.

There are now separate Application Images for applications such as Instant Messaging and Presence.

When you have navigated to the **SOFTWARE LOADS** page **BROWSE** to the ".nai" file and when ready click the **ADD LOAD** button to move it to the Primary UCM or Deployment Server.

The file can be uploaded from the Client PC you are logged in from or copied across from the RMD device (either USB or Compact Flash card) of the CPPM card as here where its being copied from the USB stick.


UCM Deployment Manager
Help | Logout
Managing: DEPLOYMENT MANAGER
User Information
Primary Server User Configuration
Please provide the details of the user account which has enough permissions for registering the backup and member server in UCM security domain.
This details will be saved in Deployment manager and will not be prompted until the provided user account exists and the password is not expired.
Primary Security server user ID: admin
Primary Security server password:
AVAYA
UCM Deployment Manager
Managing: DEPLOYMENT MANAGER
Software Loads
Software to be deployed must first be uploaded to the Deployment Manager library.
Select software load location: Deployment Server
Select media: USB Device
Browse
Specify software load file: cs1000-linux-75017-P100-M00.nai
Add Load
Delete
No software load is available to deploy or upgrade the target servers.
Please add a new software load.
Login to the UCM and navigate to SOFTWARE DEPLOYMENT . The first time you do this you will be asked for the account for registering other servers.
Once the page is displayed select SOFTWARE LOADS and UPLOAD the "NAI" file
105

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

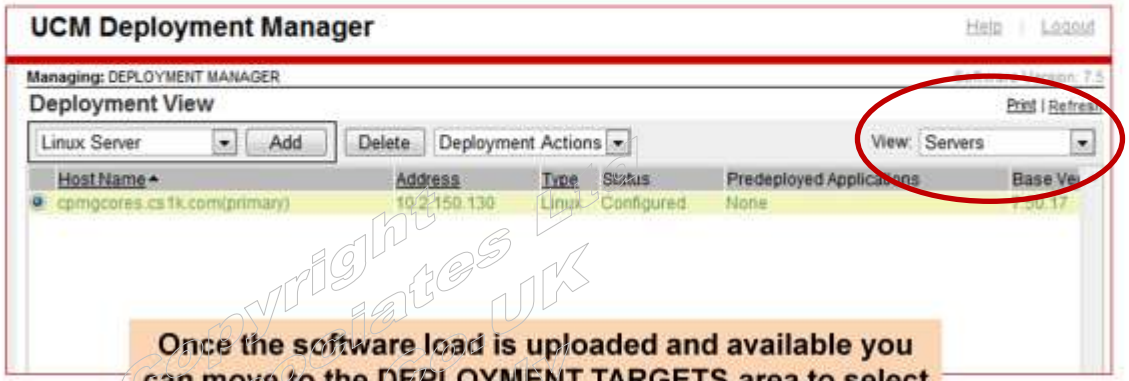
Deployment Target

Once the load is available on the UCM server you can start to deploy the servers in the Network.

Because we have installed the Linux directly onto the Server it will show up as shown in the Deployment View as a Linux Server only with no Pre Deployed Applications.

The next step is to PREDEPLOY the applications required on the server.

Use the VIEW drop down menu (Far right) to select between CS1000 systems and Network Services.



Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

106

Notes

_____

_____

_____

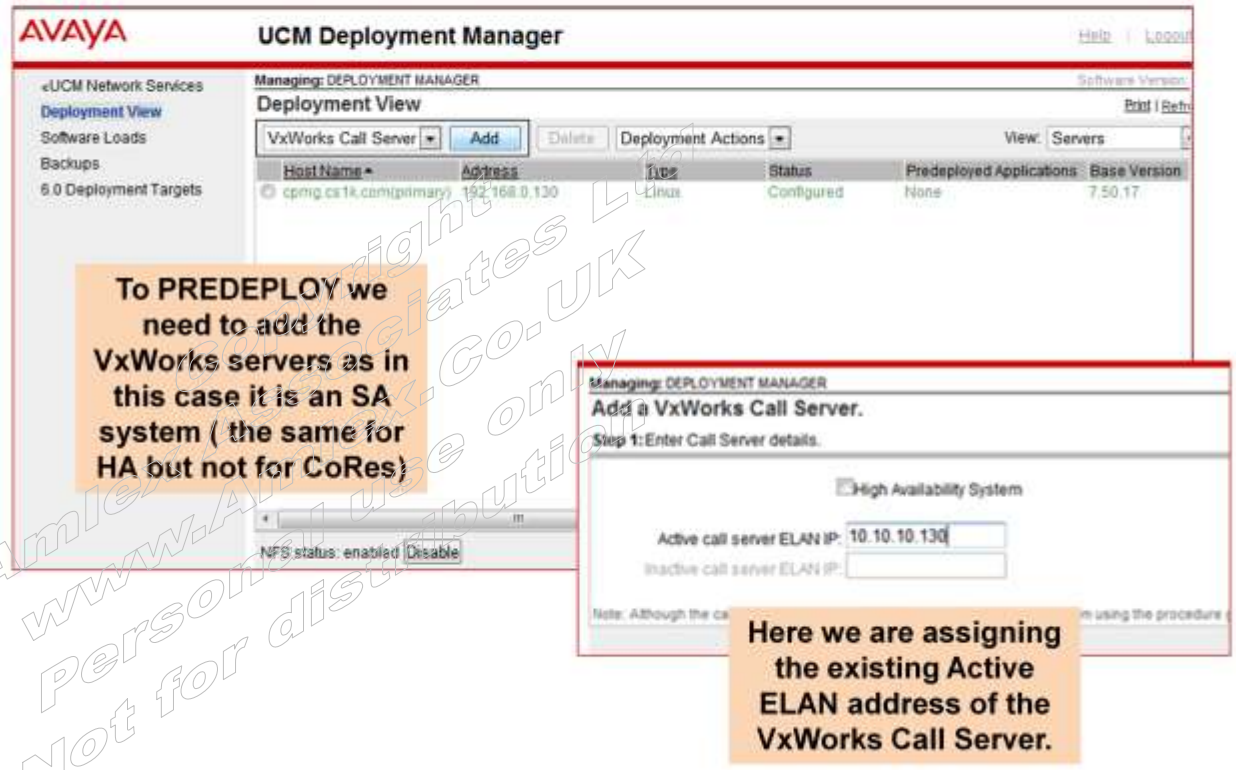
_____

Add the CS to UCM Deployment

With both the VxWorks Call server and UCM Linux servers installed and the basic configuration done (i.e. IP address on Call Server, Security Configuration on Linux) you can proceed to Deploy the Linux server as a Signalling Server and Element Manager for the Call server.

One you have logged into the UCM and added the Deployment load you will see that the Linux Server is already available to deploy. However if you are building an SA or HA configuration you need to add the VxWorks Call server(s) to the Deployment View so you can make the appropriate associations.

Select VxWorks Call Server from the drop down menu and click **ADD** as shown. You will be prompted to add the Call Server ELAN IP address and to select whether or not it is a HA system. If it is HA then the Inactive Call Server ELAN IP dialogue box will become active.



Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

107

Notes

_____

_____

_____

_____

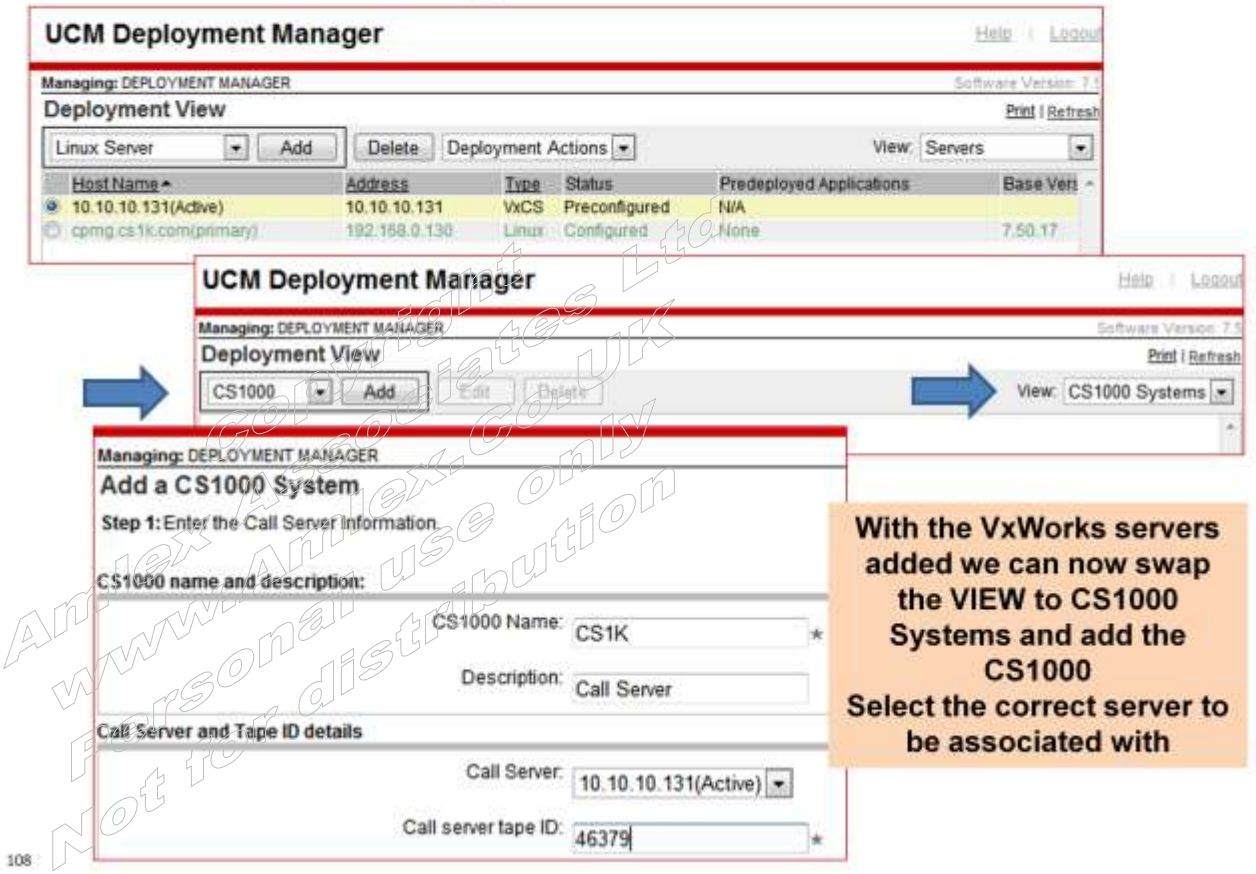
Copyright Amlex Associates Ltd

Configure Call Server

The next step is to change the View to CS1000 Systems and to add a CS1000.

You are prompted to add a Name and description and select the Call server from the drop down list as shown. Remember if you have added an HA system you will have both an Active and Inactive IP address and you should select the Active one.

You will also need to enter the Tape ID which can be printed in LD 22 of the call server. This is to ensure a correct link between the systems.



Amlex Associates Ltd www.Amlex.co.UK Confidential Personal use only Not for distribution

Notes

_____

_____

_____

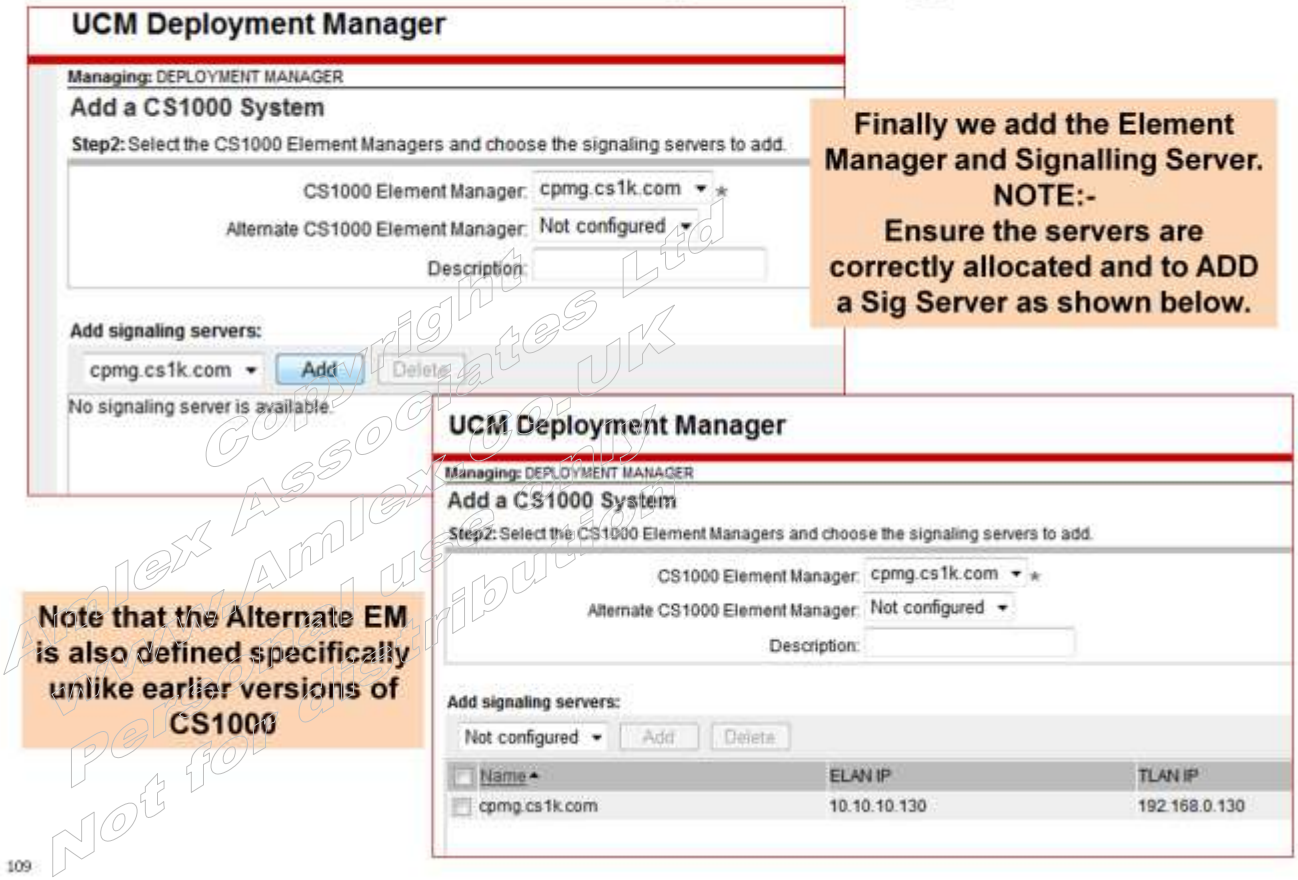
_____

Copyright Amlex Associates Ltd

Add Element Mgr & Sig Server

The next step is to add the Linux server which will provide the Element Manager for the system and then the Signalling Server.

This is done by selecting the correct server (or servers) from the drop down menu and clicking the **ADD** button



Copyright Amlex Associates Ltd
Personal use only
Not for distribution

Notes

_____

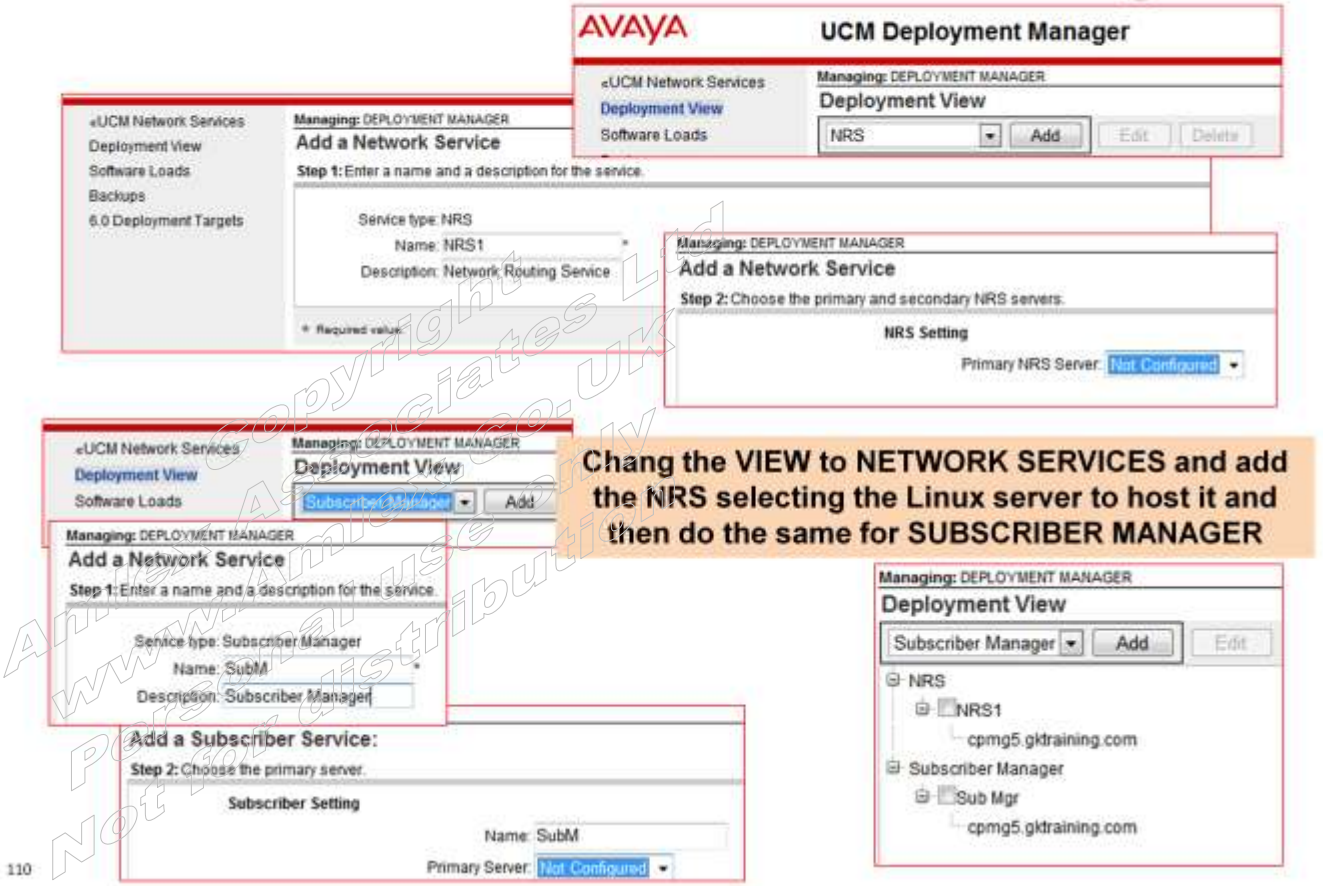
_____

_____

_____

Add NRS & Subscriber Manager

Once the Call Server elements are configured we can then add any Network Services such as the NRS (Network Routing Service) and the Subscriber Manager.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

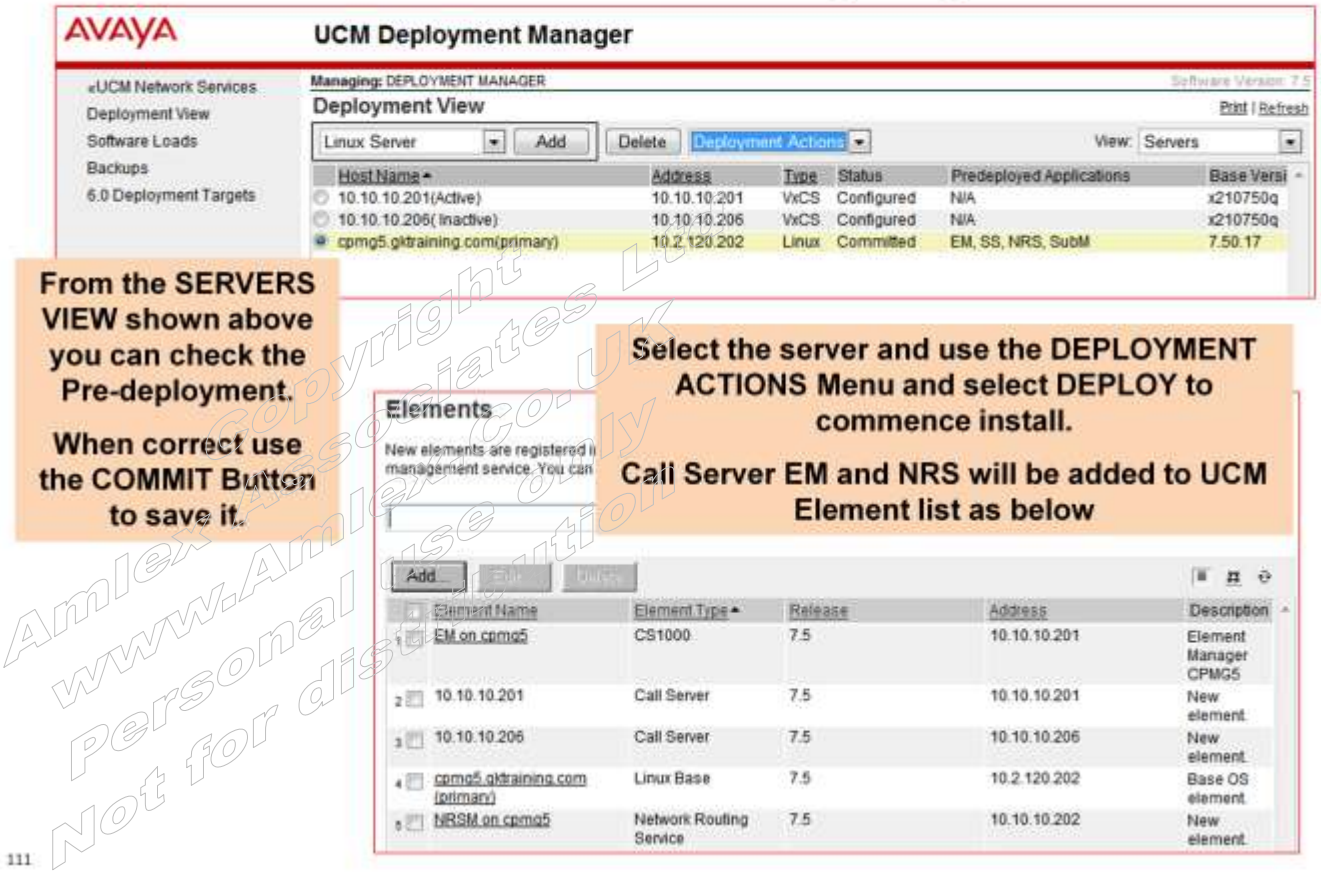
Commit & Deploy

Once the Network Services such as the NRS and Sub Manager are added we can COMMIT the Pre Deployment ready for Deployment.

In the lower screen shot you can now see the Call Server element and the Linux Server, which has the EM, SS and NRS as Predeployed Applications.

The system will now allow us to Deploy the Linux server. Once that has completed the NRS, Call Server and Element Manager will appear in the UCM Elements list and you can continue to configure the System as normal via the Command line and Element Manager.

Remember that as the CS is standalone not a CoRes CSCONSOLE will not work but CSLOGIN will and you can also connect to overlays using SSH (PuTTY) to the ELAN IP address.


AVAYA
UCM Deployment Manager
«UCM Network Services
Deployment View
Software Loads
Backups
6.0 Deployment Targets
Managing: DEPLOYMENT MANAGER
Deployment View
Print | Refresh
Linux Server
Add
Delete
Deployment Actions
View: Servers
Host Name
Address
Type
Status
Predeployed Applications
Base Versi
10.10.10.201(Active) 10.10.10.201 VxCS Configured N/A x210750q
10.10.10.206(Inactive) 10.10.10.206 VxCS Configured N/A x210750q
cpmg5.gktraining.com(primary) 10.2.120.202 Linux Committed EM, SS, NRS, SubM 7.50.17
From the SERVERS VIEW shown above you can check the Pre-deployment.
When correct use the COMMIT Button to save it.
Select the server and use the DEPLOYMENT ACTIONS Menu and select DEPLOY to commence install.
Call Server EM and NRS will be added to UCM Element list as below
Elements
Add
Element Name
Element Type
Release
Address
Description
EM on cpmg5 CS1000 7.5 10.10.10.201 Element Manager CPMG5
10.10.10.201 Call Server 7.5 10.10.10.201 New element
10.10.10.206 Call Server 7.5 10.10.10.206 New element
cpmg5.gktraining.com (primary) Linux Base 7.5 10.2.120.202 Base OS element
NRSM on cpmg5 Network Routing Service 7.5 10.10.10.202 New element
111

Notes

_____

_____

_____

_____

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

9. Adding Media Gateway

- Media Gateways
  - Up to 50 per system
  - 2 Media Gateways per Superloop (Shelf 0 & 1)
  - MG's House
    - IPE (Intelligent Peripheral Equipment) cards
    - CPPM Cards Linux or Call Server
    - CPDC/CPMG Cards Linux
    - Media Cards and DSP cards
- Require a Media Gateway Controller
  - IP Addresses for ELAN & TLAN
  - Bandwidth Zone

112

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

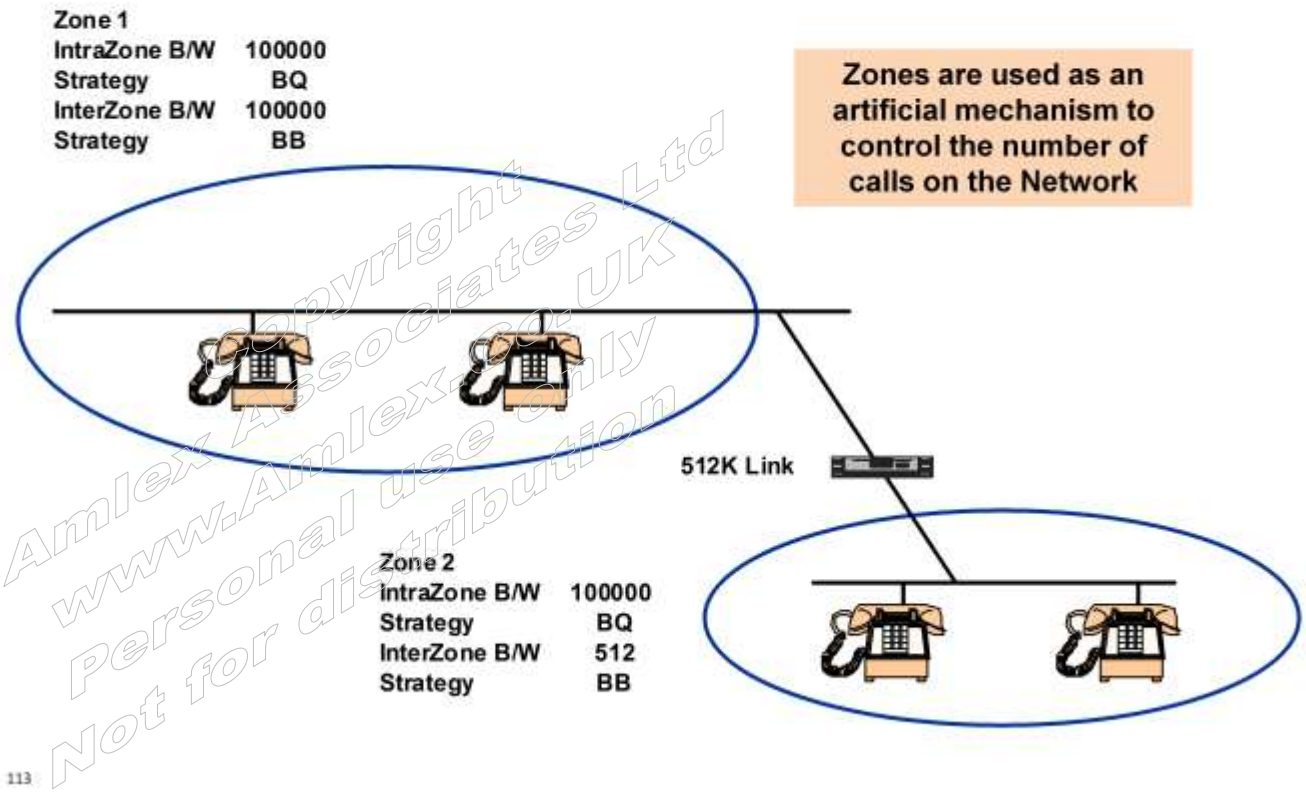
Zones are an artificial mechanism to control the number of calls made on a VoIP network. The concept is often referred to as Call Admission Control or CAC. CAC is necessary to prevent too many calls affecting call quality. In a TDM network this cannot occur as each call has its own dedicated circuit but in packet telephony we are sharing bandwidth and hence issues can occur.

If the 2 phones in zone A call each other thy have plenty of Intra zone bandwidth so the call can proceed. The system will deduct an amount of bandwidth equivalent to the calls usage from the Zone whilst the call is in place, and add it back when the call clears. Thus if there is insufficient bandwidth to allow the call it will be refused protecting the quality of other calls.

In the diagram the 2 zones have a low speed link between them of 512K. IntraZone calls will be fine but InterZone calls to Zone 1 will be more restricted.

The Strategy for calls allows us to choose a suitable codec depending on the call type. In the diagram we have selected BQ (Best Quality) for Intra Zone calls which will result in the G711 codec being used and consequently more bandwidth. However for InterZone calls we have selected BB (Best Bandwidth) which means a higher compression codec using less bandwidth will be selected if available. This will usually be G.729 and VAD (Voice activity Detection) may also be selected to save even more bandwidth allowing more calls to use the link at the same time.

Bandwidth Zones



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

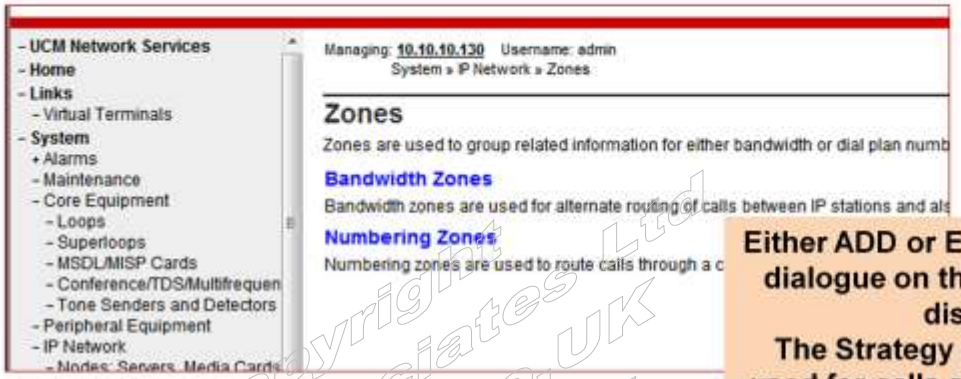
_____

Creating a B/W Zone

Bandwidth Zones can be created in LD 117 using the command
⇒NEW ZONE <zone Number>

This will create a zone with the default values which can be later edited using the Element manager.

The screenshot shows the Zone creation/editing in Element Manager.


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
- Core Equipment
- Loops
- Superloops
- MSDL/MISP Cards
- Conference/TDS/Multifrequen
- Tone Senders and Detectors
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
Managing: 10.10.10.130 Username: admin
System » IP Network » Zones
Zones
Zones are used to group related information for either bandwidth or dial plan numb
Bandwidth Zones
Bandwidth zones are used for alternate routing of calls between IP stations and als
Numbering Zones
Numbering zones are used to route calls through a c

Either ADD or EDITthe Zone and the dialogue on the next page will be displayed.
The Strategy defines the Codec used for calls and the bandwidth is used to calculate the maximum number of calls.

	Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BQ	1000000	BQ	SHARED	MO	
2	5	1000000	BQ	1000000	BQ	SHARED	BMG	
3	10	1000000	BQ	1000000	BQ	SHARED	VTRK	

114

Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

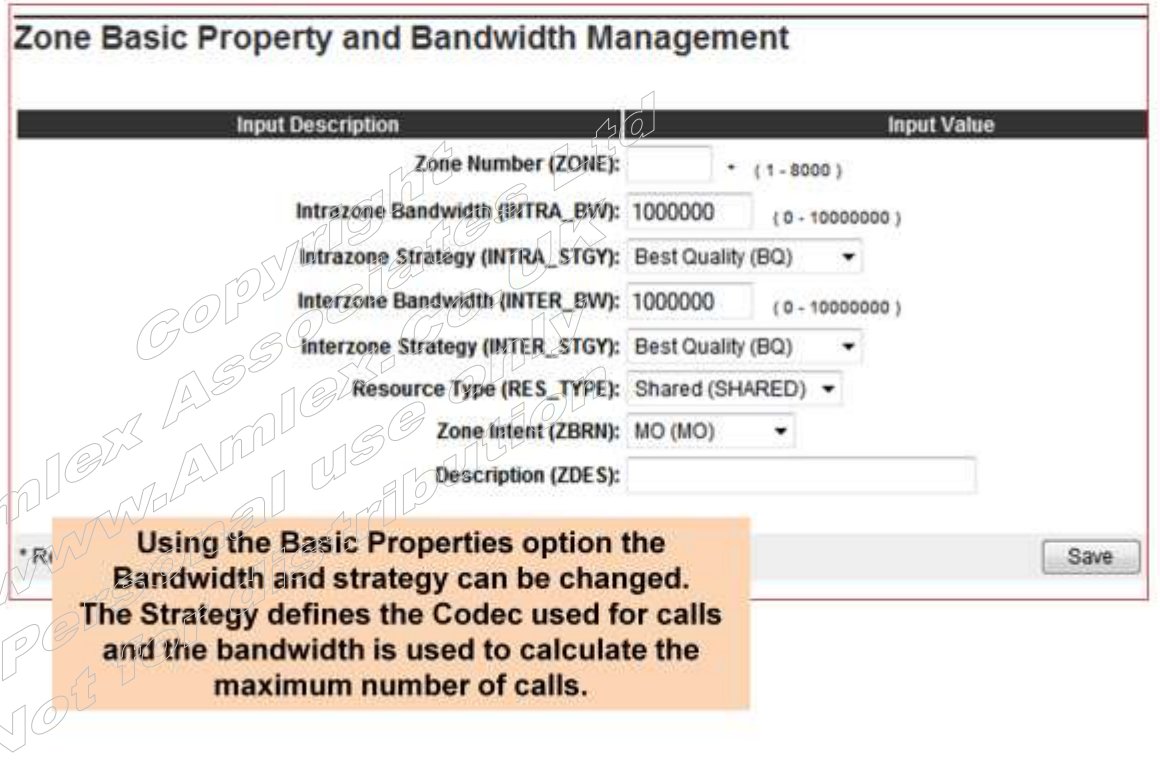
_____

Copyright Amlex Associates Ltd

Bandwidth Zone Properties

Here we can define how much bandwidth is available for calls in each zone allowing us to control them.

In addition Zones can select the Codec to use for calls (Controlling the compression etc.) based on the Strategy setting for both Intra and Inter zone calls.


Zone Basic Property and Bandwidth Management
Input Description
Input Value
Zone Number (ZONE):
(1 - 8000)
Intrazone Bandwidth (INTRA_BW):
1000000
(0 - 10000000)
Intrazone Strategy (INTRA_STGY):
Best Quality (BQ)
Interzone Bandwidth (INTER_BW):
1000000
(0 - 10000000)
Interzone Strategy (INTER_STGY):
Best Quality (BQ)
Resource Type (RES_TYPE):
Shared (SHARED)
Zone Intent (ZBRN):
MO (MO)
Description (ZDES):
Save
Using the Basic Properties option the Bandwidth and strategy can be changed. The Strategy defines the Codec used for calls and the bandwidth is used to calculate the maximum number of calls.
115

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Add Media Gateway

The basic assignment of the IP address to the Media Gateway can be done in LD 97.

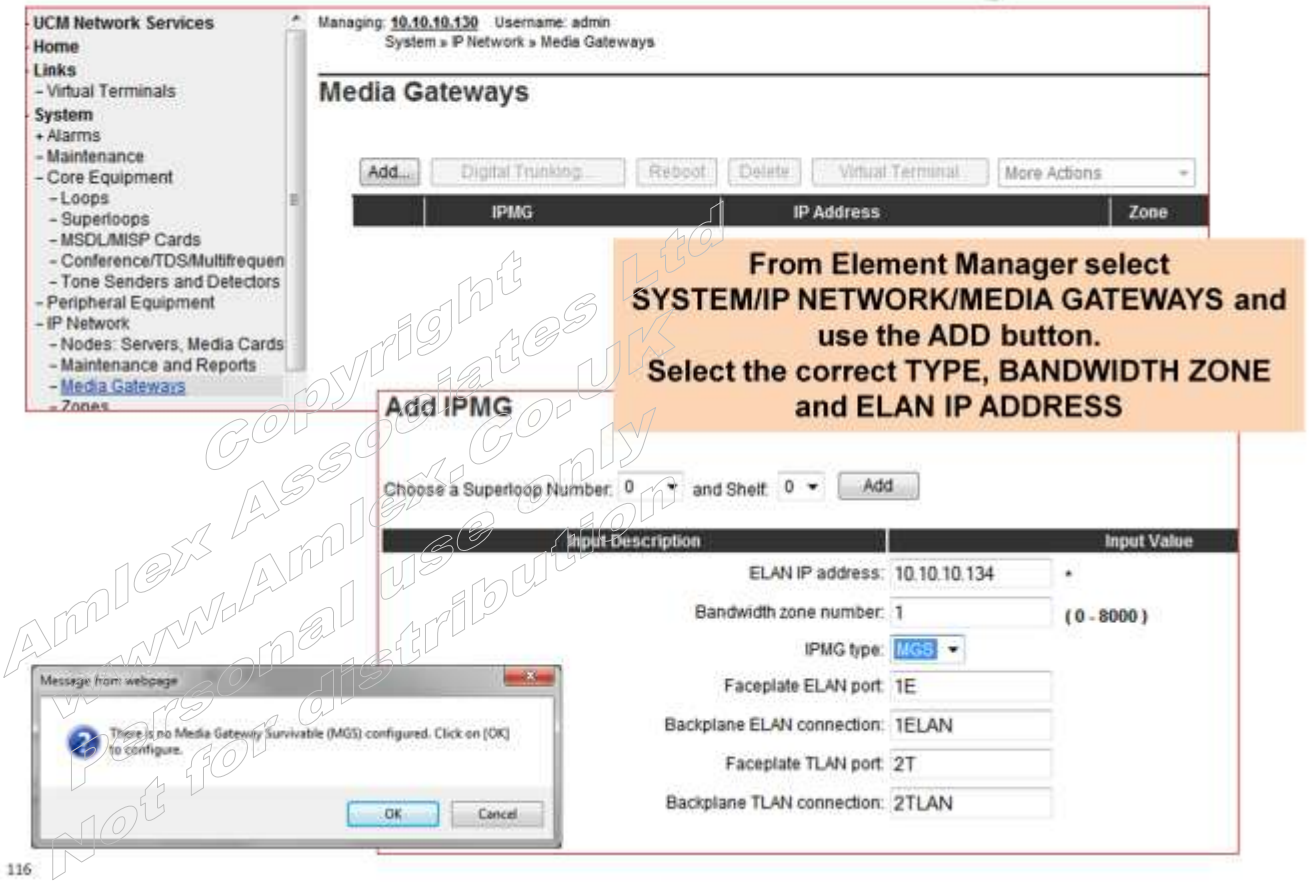
However the full configuration of DSP cards etc must be completed in Element manager so the example shows the complete configuration in EM.

First we define the Superloop and Shelf number for the IP Media Gateway (IPMG).

Then we add the ELAN IP address of the Media Gateway and the Zone number it will be placed in. Note that whilst the screen shows that the Zone can be from 0-255 you should only ever use Zone 0 for Soft Phone sets if at all as it will cause issues.

Clicking OK on the popup dialogue will take you to the next screen where the DSP configuration can be added.

NOTE:- the ADD IPMG Dialogue shows the addition of an MGS (from a CPMG card) and hence shows less Ports (Faceplate/Backplane etc) than would be seen when configuring an MGC card.



Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

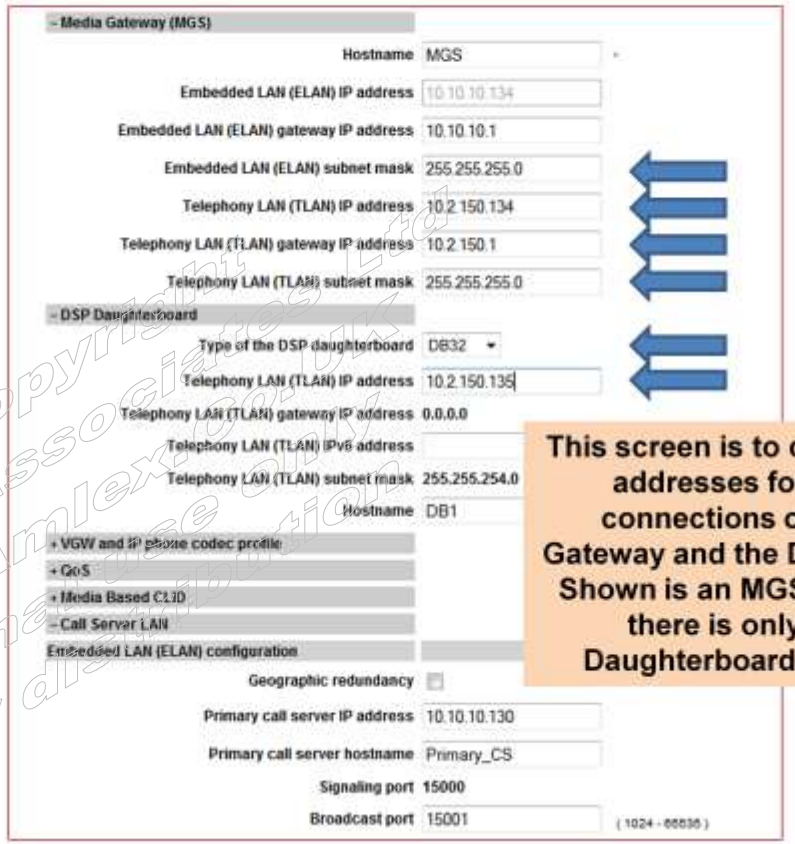
_____

DSP Daughter Boards

Having clicked OK to add the full Media Gateway configuration we are prompted as shown to add the IP addressing etc for the rest of the card including the DSP channels.

Here we are adding the information regarding he DSP daughter board hosted on this MGS and the TLAN information.

NOTE:- When you scroll down you will find the section regarding Primary Call Server under the ELAN Tab. Here the Call server is defined automatically but it is worth checking for mistakes. Also Note the Geographic Redundancy tick box which is used when a Survivable Media Gateway is configured . Once this is enabled you will be offered options to add the active call server addresses for the Alternate Call Servers.


- Media Gateway (MGS)
Hostname MGS
Embedded LAN (ELAN) IP address 10.10.10.134
Embedded LAN (ELAN) gateway IP address 10.10.10.1
Embedded LAN (ELAN) subnet mask 255.255.255.0
Telephony LAN (TLAN) IP address 10.2.150.134
Telephony LAN (TLAN) gateway IP address 10.2.150.1
Telephony LAN (TLAN) subnet mask 255.255.255.0
- DSP Daughterboard
Type of the DSP daughterboard DB32
Telephony LAN (TLAN) IP address 10.2.150.135
Telephony LAN (TLAN) gateway IP address 0.0.0.0
Telephony LAN (TLAN) IPv6 address
Telephony LAN (TLAN) subnet mask 255.255.254.0
Hostname DB1
+ VGW and IP phone codec profile
+ QoS
+ Media Based CLID
- Call Server LAN
Embedded LAN (ELAN) configuration
Geographic redundancy
Primary call server IP address 10.10.10.130
Primary call server hostname Primary_CS
Signaling port 15000
Broadcast port 15001
(1024 - 65535)

This screen is to configure the IP addresses for the TLAN connections of the Media Gateway and the Daughter board. Shown is an MGS which is why there is only one DSP Daughterboard to configure

Copyright Amlex Associates Ltd
www.Amlex.com UK
Personal use only
Not for distribution

117

Notes

_____

_____

_____

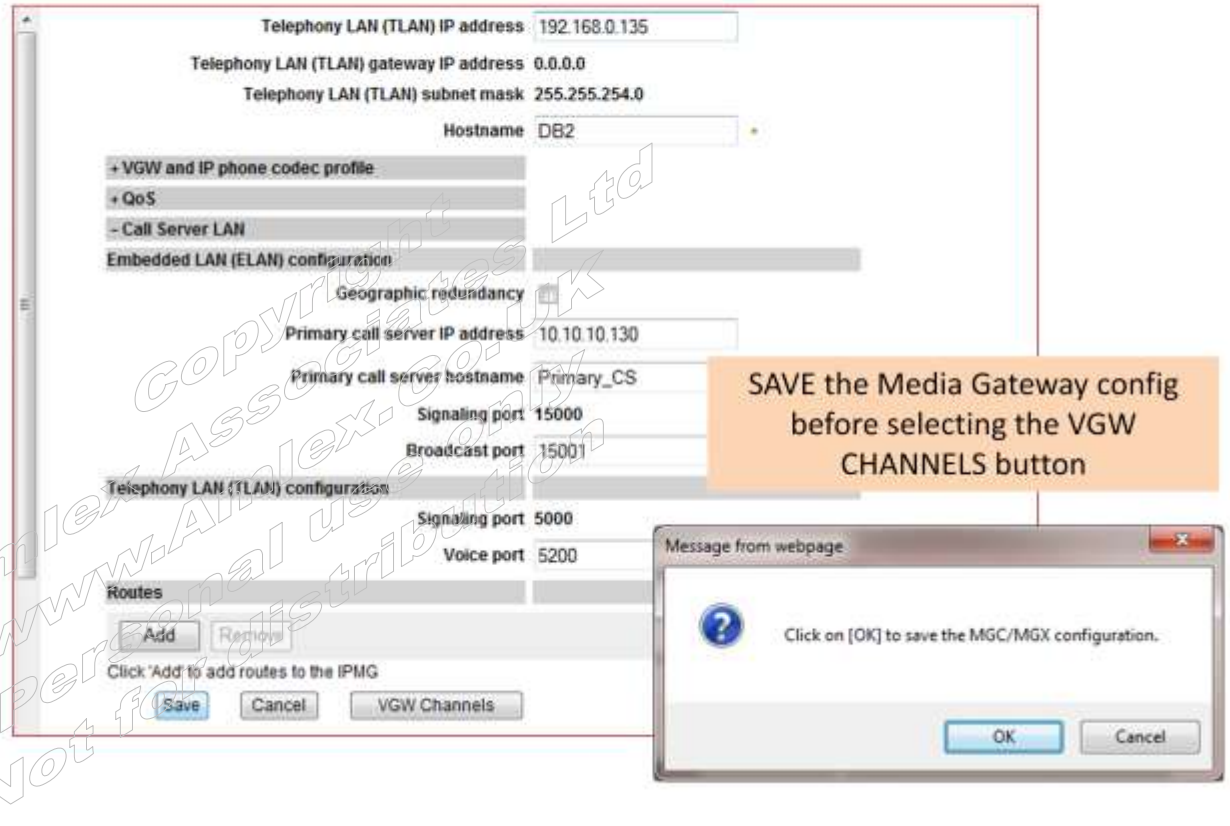
_____

Full MGC/MGS Configuration

Scrolling down the page we can access the fields for the Primary Call server address. This should be pre populated but do check it is correct before saving the configuration.

DO NOT click the **VGW CHANNELS** button before saving or all the data will be lost.

Note that if the GEOGRAPHIC REDUNDANCY tick box is selected more fields will be displayed for adding the Alternate Call Server addresses for Triple Registration of the MGC.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

118

Notes

_____

_____

_____

_____

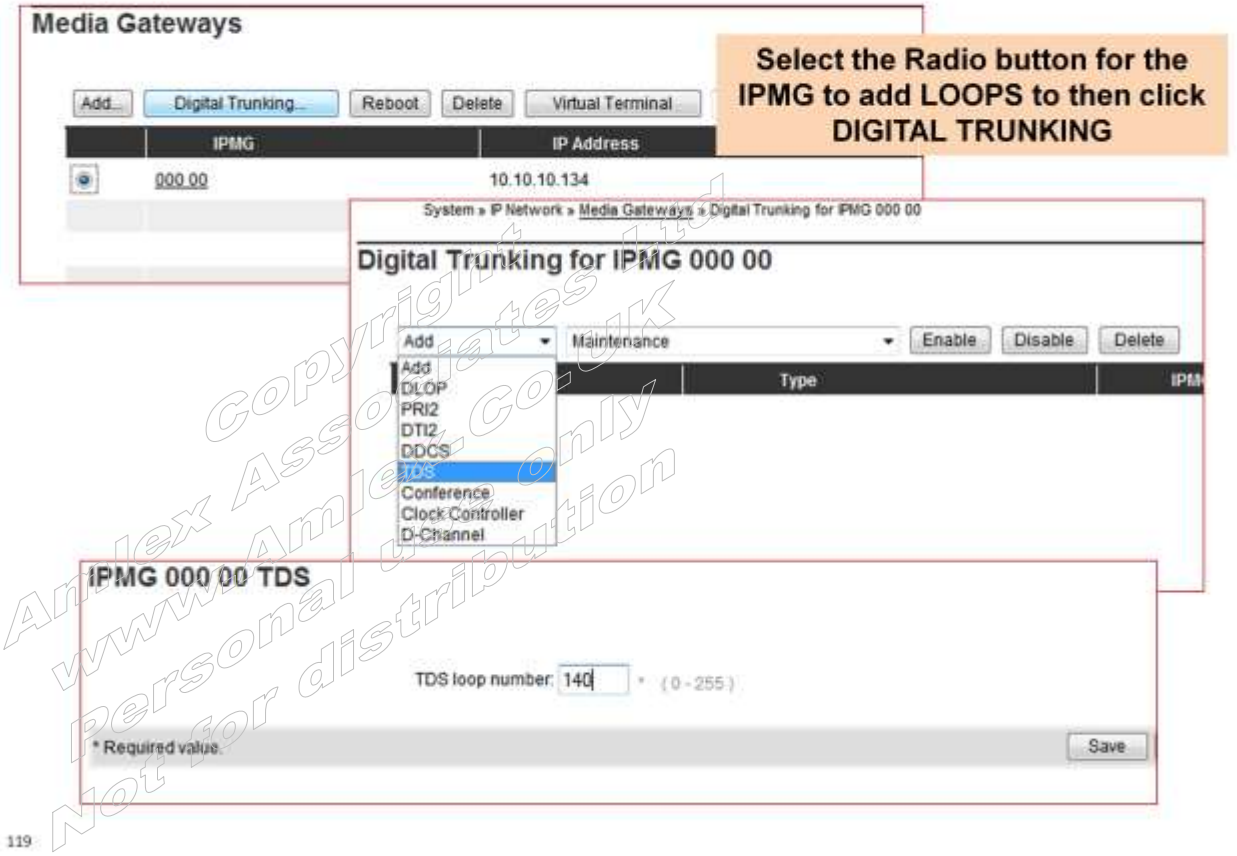
Copyright Amlex Associates Ltd

Adding TDS & Conference Loops

Media Gateways need to have Tone & Conference loops assigned to them, and a maximum of two of each is allowed . Each Conference loop supports 30 circuits giving 60 in total per media gateway.

Select the Radio button for the IPMG to add LOOPS to then click **DIGITAL TRUNKING** to access the lower screen and add the TDS and Conference loops.

Use Loop numbers which don't conflict with the current configuration. Possibly Loops 140-143 etc.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

VGW Channels – Card Allocation

Before adding the VGW channels we need to understand how they are organised.

The diagram shows how the cards in the Media Gateway are arranged and addressed by the system.

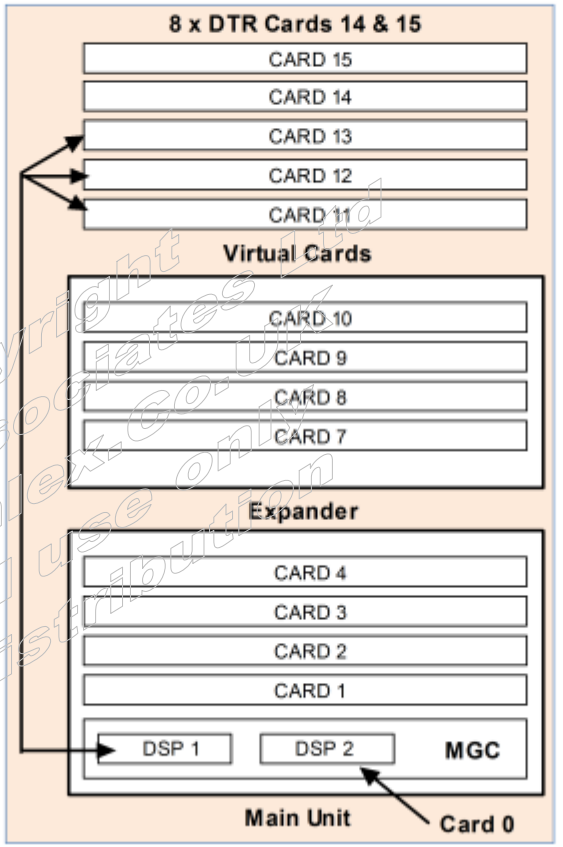
As well as the eight physical card slots there are “Virtual” cards as shown (slot 0 and Slots 11-15). These are used to address the DSP daughterboard cards and also the Digitone Receivers required on the Media Gateway.

In Release 5&6 with the DSP 32 & DSP96 cards slot assignment was as follows but the 128 Port DSP has changed this See Page 29 for 128 Port card assignments.

DSP Daughter Board 1 Cards 11,12 & 13

DSP Daughter Board 2 Card 0

Digitone Receivers Cards 14 & 15 (8 per card units 0-7)



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

120

Notes

_____

_____

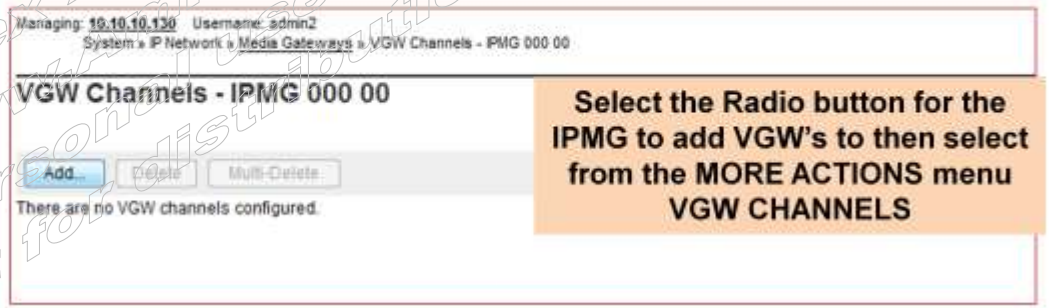
_____

_____

VGW Channels - TDM to IP

The Voice Gateway Channels for TDM to IP conversion can be added to the system by selecting the media gateway (Radio button) and then selecting **VGW CHANNELS** from the **MORE ACTIONS** drop down menu.

This will display the Add screen shown . Clicking the **ADD** button will display a screen for configuring the channels. (See over)


Managing: 10.10.10.130 Username: admin2
System » IP Network » Media Gateways » VGW Channels - IPMG 000 00
VGW Channels - IPMG 000 00
Add...
Delete
Multi-Delete
There are no VGW channels configured.
Select the Radio button for the IPMG to add VGW's to then select from the MORE ACTIONS menu VGW CHANNELS

121

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

VGW Channels

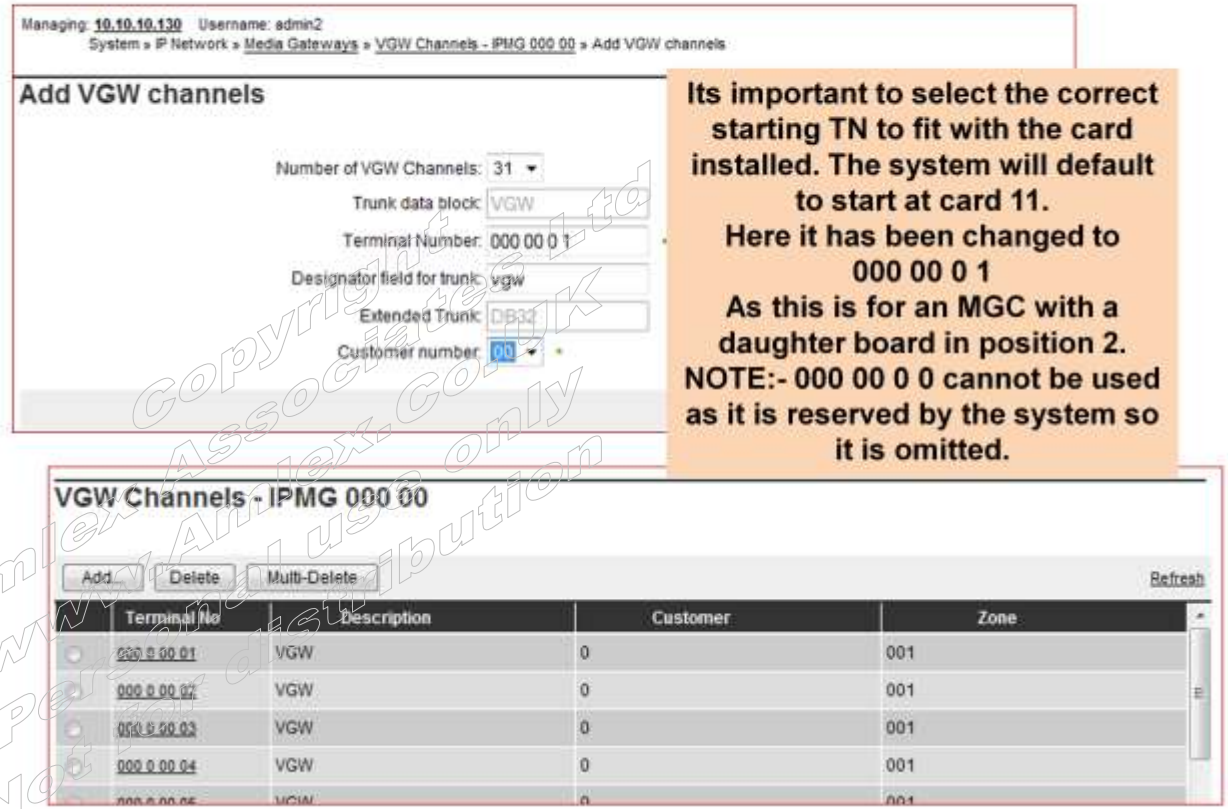
The ADD VGW CHANNELS dialogue shown will default to the Media Gateway Loop and Shelf followed by Card 11 as it expects position 1 to be used.

In the example shown herewe have a 32 port card in position 2 but this causes an issue as the first TN for the card would be :-
000 00 0 0

However this is reserved for system use so in this instance we will have to lose the first VGW channel and only add 31 units starting at TN 000 00 0 1. This is only an issue on IPMG 0 0.

The lower screen shows the configured channels .

On a CPMG card the MGS has its fixed DSP ports on Card 11 so if used as IPMG 0 the same problem does not occur.


Managing: 10.10.10.130 Username: admin2
System » IP Network » Media Gateways » VGW Channels - IPMG 000 00 » Add VGW channels
Add VGW channels
Number of VGW Channels: 31
Trunk data block: VGW
Terminal Number: 000 00 0 1
Designator field for trunk: vgw
Extended Trunk: DB32
Customer number: 00
Its important to select the correct starting TN to fit with the card installed. The system will default to start at card 11.
Here it has been changed to 000 00 0 1
As this is for an MGC with a daughter board in position 2.
NOTE:- 000 00 0 0 cannot be used as it is reserved by the system so it is omitted.
VGW Channels - IPMG 000 00
Add
Delete
Multi-Delete
Refresh
Terminal No
Description
Customer
Zone
000 0 00 01 VGW 0 001
000 0 00 02 VGW 0 001
000 0 00 03 VGW 0 001
000 0 00 04 VGW 0 001

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

122

Notes

_____

_____

_____

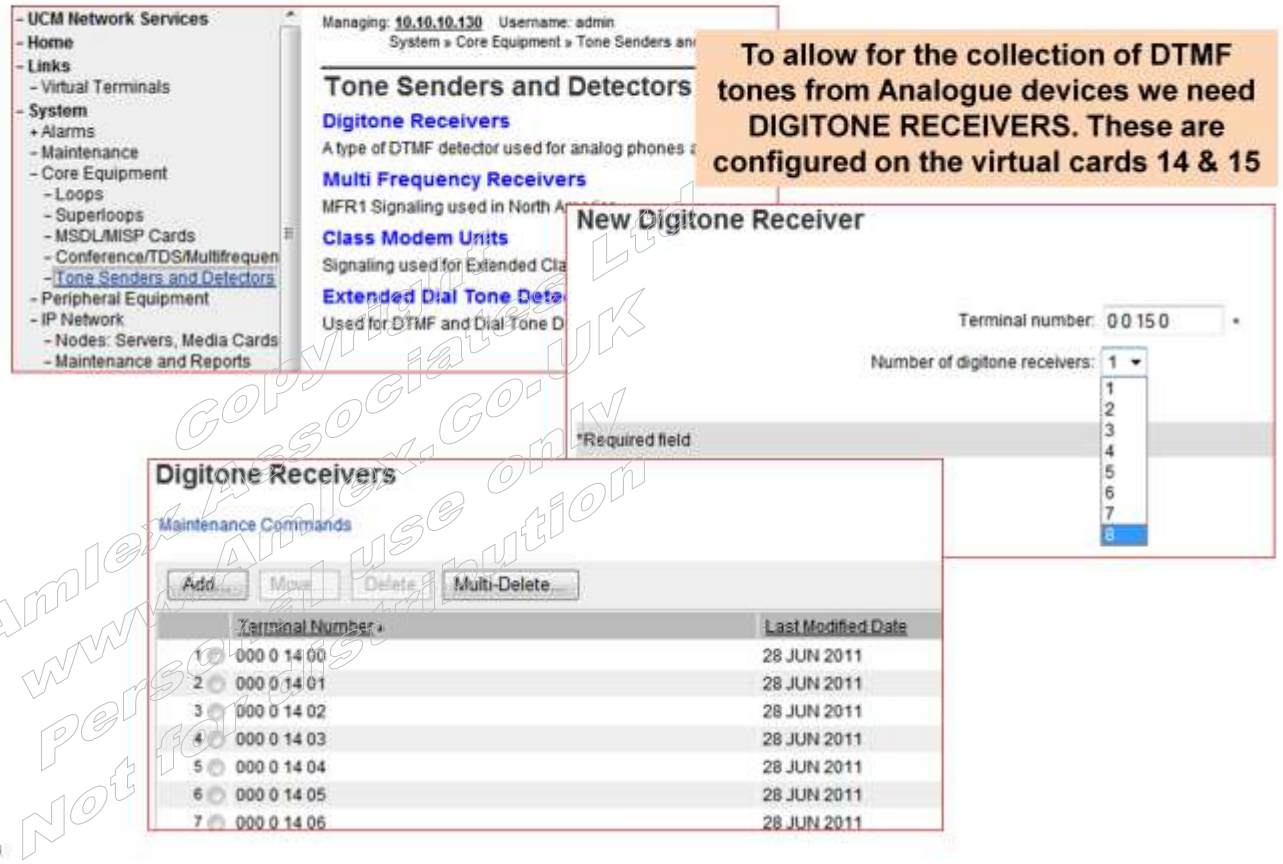
_____

Add Multiple Digitone Receivers

Digitone receivers (DTR's or XTD's) are required to interpret the DTMF dialling from analogue sets registered to the Media Gateway.

The functionality is hosted on the MGC/MGS on the virtual cards as described earlier. The DTR's can be configured through the Element Manager or via LD 13.

The Add screen is shown here and we can add all eight in one step . Note some systems may use XTD (Extended Tone Detectors) rather than DTR devices .



Amlex Associates Ltd
Copyright
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add IP Addresses to MGC/MGS

Once the Media Gateway is configured into the Element Manager you need to configure the actual MGC with IP addresses so it can communicate with the call server and the rest of the system.

To do this on a new card or one that has been cleared you simply need to power it on with a terminal connected to the Console port 0 of the card. If there are no IP addresses configured the card will automatically run "mgcsetup" which will prompt you for the relevant information.

The advanced parameters are used to configure the ELAN & TLAN ports and to select ELAN security. Intra System Signalling Security is based on the IPsec protocol and is used on the ELAN to protect the signalling between different devices. Ensure you build your system and ensure it is working correctly before attempting to use ISSS.

124

In the event that the MGC/MGS encounters problems and needs to be cleared, see the APPENDIX – MGC/MGS COMMANDS for procedures.

- MGC Card needs IP addresses to register with CS
- If card is new or cleared mgcsetup is initiated automatically
- Card should reboot with new addresses and register with CS
  - Downloads updates to Loadware
- Addresses can be cleared or changed
  - mgcIPClear
    - Clears IP Addresses stored in NVRam on card
  - mgcsetup
    - Add IP Addressing to card
  - diskformat
    - Formats Compact Flash card removing any stored Passwords and upgraded loadware

Dialogue from Console Port of MGC/MGS

```
ELAN IP                 : 10.10.10.14
ELAN subnet mask        : 255.255.255.0
ELAN gateway IP         : 10.10.10.1
Primary CS IP           : 10.10.10.11
Change MGC advanced parameters? (y/[n]) : y

TLAN is set to auto negotiate, change? (y/[n]) :
ELAN is set to auto negotiate, change? (y/[n]) :
ELAN security Disabled, change? (y/[n]) :

You have entered the following parameters for this MG
      1000E:

ELAN IP           : 10.10.10.14
ELAN subnet mask  : 255.255.255.0
ELAN gateway IP   : 10.10.10.1
Primary CS IP     : 10.10.10.11
TLAN set to auto negotiate.
ELAN set to auto negotiate.
ELAN security Disabled
Is this correct? (y/n/[a]bort) : y
```

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution Confidential

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

MGC Boot Up Registration to CS

In the event the MGC is configured with the wrong address and you need to change it using mgcsetup you will need to gain access to the card.

If the card has not downloaded the loadware updates from the call server you cannot use <CTRL> LDB or <CTRL>OAM to login so you need to use the <CTRL i> option shown here on the boot dialogue.

In this instance all is well and the card has registered to the call server and as you can see is preparing for an upgrade of the cards Loadware.

```
FPGA VERSION is 41413135 AA15
MGC GOLD Image
MGCCAL63 Friday May 08 2009 08:22:53 EDT
Failed to read Tlan IP address information from bootline.

 *** To invoke install menu or bypass loadware upgrade enter CONTROL-I ***
Init ISEC succeeded
Registered successfully to Primary Call Server[10.10.10.130]
Received configuration data from Primary Call Server on attempt[1]
Received an upgrade request. Preparing IPMG for upgrade.

MGC Superloop and Shelf information not available.
0x83fdef50 (tMGCInst): Cabinet Number not available.Retrying to obtain the cabinet
    number...
logTask: 2 log messages lost.
OMM: IP link is UP between Primary Call Server and IPMG[0 0]
Failed to read Tlan IP address information from bootline.
....
 Bootline stored in NV_RAM
.................
```

125

Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution Copyright

Notes

_____

_____

_____

_____

Call Server MGC Registration

This diagram shows the Call server messages for the MGC registration and the detection of the Loadware mismatch.

This is because the MGC uses its simple Gold image to boot up and then downloads the Loadware updates from the call server saving then locally on the 128Mb Compact Flash card.

On subsequent restarts of the card it will then boot from the Compact flash images rather than the Gold image.

OVL000

>

SRPT077 IPMG[0 0]: Loadware version mismatch detected. Adding to sequential upgrade queue.

SRPT226 Registration has been granted for IP[10.10.10.134] IPMG[0 0]

SRPT017 OMM: IP link is UP between Call Server and IPMG[0 0]

----- AFTER MGC HAS UPGRADED ------

AUD000

SRPT077 Centralized Software Upgrade complete.

SRPT016 OMM: IP link is DOWN between Call Server and IPMG[0 0]

126

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

MGC Centralised S/W upgrade

Here are the MGC upgrade messages as the Loadware is upgraded from the call server.

Note that the MGC will reboot after the upgrade to enable the new loadware.

```
....
 Bootline stored in NV_RAM
.....Auto commit option has been enabled.
Upgrade of CSP loadware initiated.
Upgrade of MSP loadware initiated.
Upgrade of APP loadware initiated.
Upgrade of DBL2 initiated.
0x83fdef50 (tMGCInst): Upgrading Application Loadware ...
0x83fdef50 (tMGCInst): Gold CSP image upgraded
0x83fdef50 (tMGCInst): mgcBootLineFix:fixing the bootline
0x83fdef50 (tMGCInst): Upgrade Application Loadware
   completed
Upgrade completion message has been sent successfully.
0x83fdef50 (tMGCInst): Rebooting MGC to take the upgrade in
   effect.
/e/  - Volume is OK
```

127

Amlex Associates UK
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

AVAYA
Communications Server 1000
Release 7.5

Part 2

Installation, Configuration,
Support & Troubleshooting

Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

128

Unified Communications Manager

The UCM framework adds a complete management and Security Domain to the CS1K environment.

It controls access to the systems and servers as well as regulating communications between them.

When the component devices are initially configured (Call Server, Media Gateway etc) they are outside of the UCM domain but can communicate at a basic level. For full functionality however they must be added to the UCM domain. This is done in one of two ways

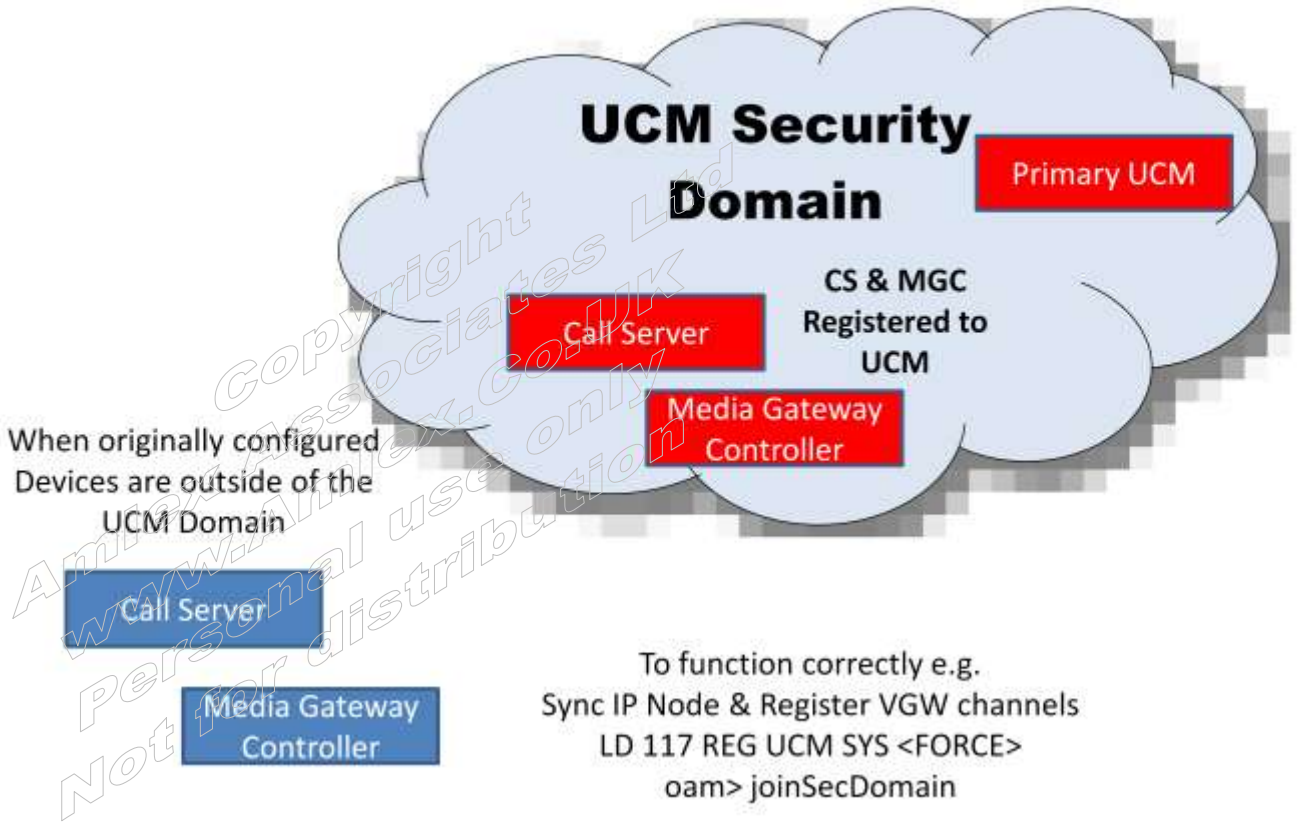
LD 117 REG UCM SYS

Or on the command line of the device e.g. MGC card

oam> joinSecDomain

These commands complete the registration of the devices to allow SSH communications between them. Specifically IP Node synchronisation and MGC configuration download.

10. Joining the UCM Security Domain


UCM Security Domain
Primary UCM
CS & MGC Registered to UCM
Call Server
Media Gateway Controller
When originally configured Devices are outside of the UCM Domain
Call Server
Media Gateway Controller
To function correctly e.g.
Sync IP Node & Register VGW channels
LD 117 REG UCM SYS <FORCE>
oam> joinSecDomain

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

129

Notes

In order to add both the Call Server and MGC to the UCM Domain we can issue the command REG UCM SYS in LD 117.

This first of all turns on Centralised Authentication so that only UCM accounts can be used to login to the call server (e.g. admin) and then it tries to add all registered elements such as MGC's to the UCM.

In this example the registration fails and on the next page you will see an alternate method of adding and MGC to the UCM.

NOTE:-

The STAT UCM INFO and STAT UCM SYS (REFRESH) commands are used to determine the UCM current status. It is important to use the REFESH option to check for the latest position as if devices are registered using joinSecDomain, their status is usually shown incorrectly if STAT UCM SYS is used.

Register UCMSecurity System

```
>LD 117
=> reg ucm sys          - register ucmsecurity system
SEC037 Security domain membership has been granted.  (Centralized authentication is now enabled.)
DONE !
IP address of the Primary Security Server: 192.168.0.130
User Name (UCM): admin
Password (admin):
These elements are registered with the Call Server
        MGC     10.10.10.134
Do you want to allow these 1 elements to request security domain membership using your credentials?
     (Y/N) [N] y
Sending messages to 1 elements authorizing them to request security domain membership.
Waiting for status updates from each of the elements...
.....
SEC102 Element 10.10.10.134 failed to request membership in the security domain, Reason
 FAILED: Upload Element Properties file failed!.
.The Call Server and 0 attached elements successfully requested security domain membership, but 1
     elements failed.
=>
=> stat ucm info
Central Authentication is enabled
The Security Domain IP address is : 192.168.0.130
The Security Domain Fingerprint is: 59:E2:47:2B:11:EE:79:34:17:F8:0E:76:5B:C6:8E:EE
=> stat ucm sys refresh
Requesting UCM registration status from devices.
Waiting for status updates from each of the elements...
No elements registered with the Call Server
```

UCM "admin" account and password

Use the STAT UCM commands to check status of elements

130

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

As the UCM registration failed for this MGC we have logged into it using the command <CTRL>OAM and the account admin2 (this works still as the MGC is outside the UCM).

Once you have accessed the OA shell issue the command

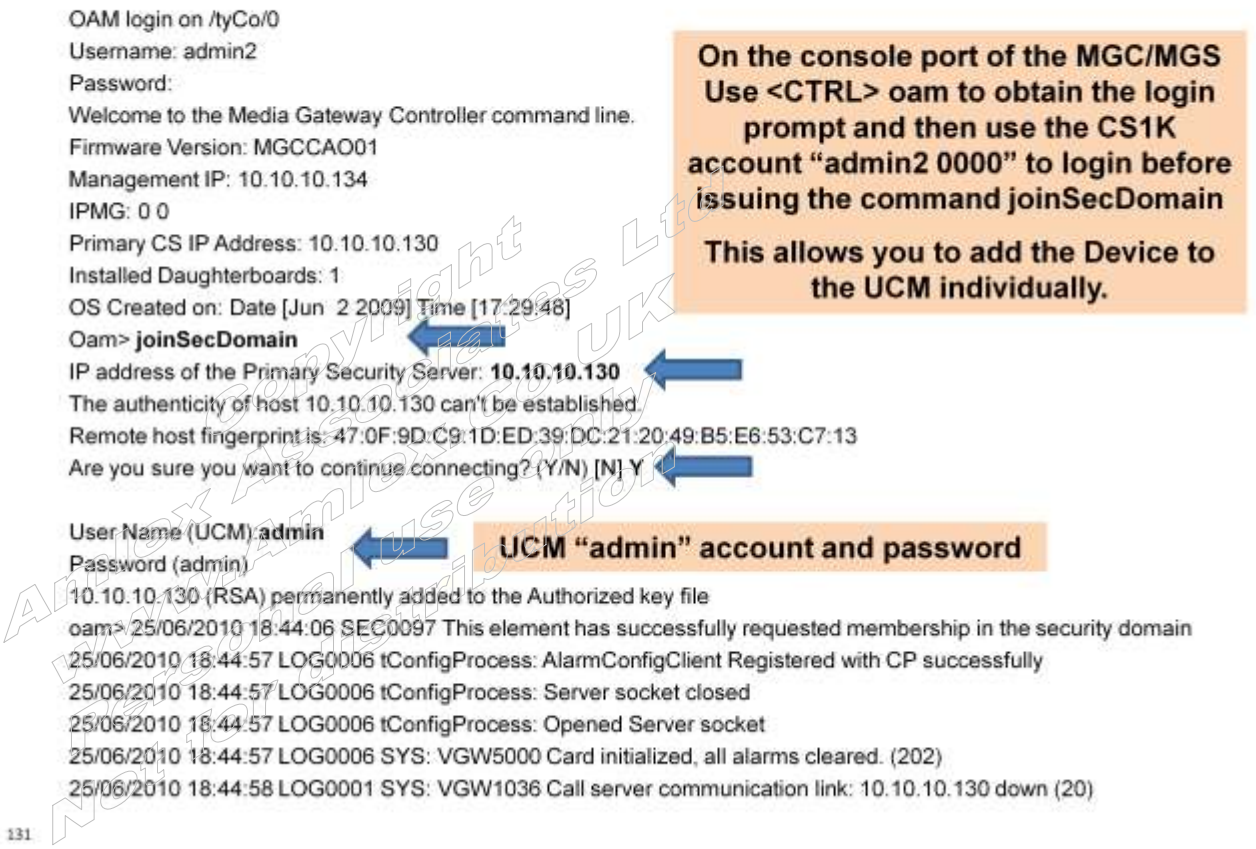
OAM> joinSecDomain

Follow the prompts for the IP address of the UCM and login details and the card will try to register itself.

As you can see this is successful and the card resets itself so full communication can be established and the VGW channels enabled.

If you now check the UCM elements list you should find that a new entry has been added for the MGC card.

JoinSecDomain


OAM login on /tyCo/0
Username: admin2
Password:
Welcome to the Media Gateway Controller command line.
Firmware Version: MGCCAO01
Management IP: 10.10.10.134
IPMG: 0 0
Primary CS IP Address: 10.10.10.130
Installed Daughterboards: 1
OS Created on: Date [Jun 2 2009] Time [17:29:48]
Oam> joinSecDomain
IP address of the Primary Security Server: 10.10.10.130
The authenticity of host 10.10.10.130 can't be established.
Remote host fingerprint is: 47:0F:9D:C9:1D:ED:39:DC:21:20:49:B5:E6:53:C7:13
Are you sure you want to continue connecting? (Y/N) [N] Y
User Name (UCM): admin
Password (admin)
10.10.10.130 (RSA) permanently added to the Authorized key file
oam> 25/06/2010 18:44:06 SEC0097 This element has successfully requested membership in the security domain
25/06/2010 18:44:57 LOG0006 tConfigProcess: AlarmConfigClient Registered with CP successfully
25/06/2010 18:44:57 LOG0006 tConfigProcess: Server socket closed
25/06/2010 18:44:57 LOG0006 tConfigProcess: Opened Server socket
25/06/2010 18:44:57 LOG0006 SYS: VGW5000 Card initialized, all alarms cleared. (202)
25/06/2010 18:44:58 LOG0001 SYS: VGW1036 Call server communication link: 10.10.10.130 down (20)
131
On the console port of the MGC/MGS Use <CTRL> oam to obtain the login prompt and then use the CS1K account "admin2 0000" to login before issuing the command joinSecDomain
This allows you to add the Device to the UCM individually.
UCM "admin" account and password

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

11. IP Telephony Node

The **Node ID** is a number of up to 4 digits used to identify the node. The **Node IP Address** is a TLAN address but not the TLAN address of the sig server itself and represents the whole node.

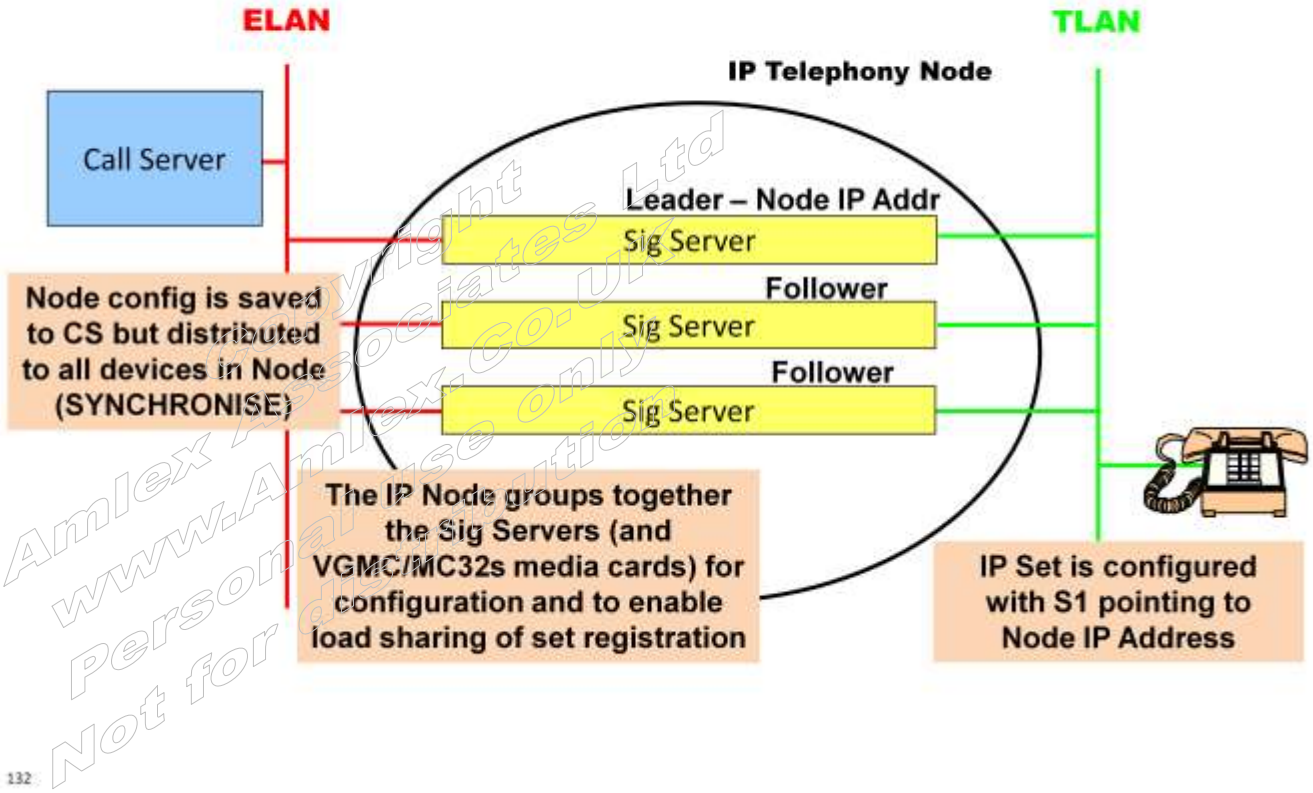
The **Node IP Address** is held by the **Leader** of the IP telephony node. This will normally be a signalling server.

Devices in the Node are either a **Leader** (one only) or **Follower**. In the event of a failure of the Leader the Followers will elect a new Leader which will then assume the Node IP address as well as its own TLAN address.

The IP sets are configured with the IP Node address, thus even in the event of a Sig server failure the IP Node address will still be available via the new **Leader.**

All of the devices running TPS are included in the IP Telephony node.

A system can have multiple IP Nodes if required.


ELAN
TLAN
IP Telephony Node
Call Server
Leader – Node IP Addr
Sig Server
Follower
Sig Server
Follower
Sig Server
Node config is saved to CS but distributed to all devices in Node (SYNCHRONISE)
The IP Node groups together the Sig Servers (and VGMC/MC32s media cards) for configuration and to enable load sharing of set registration
IP Set is configured with S1 pointing to Node IP Address
132

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

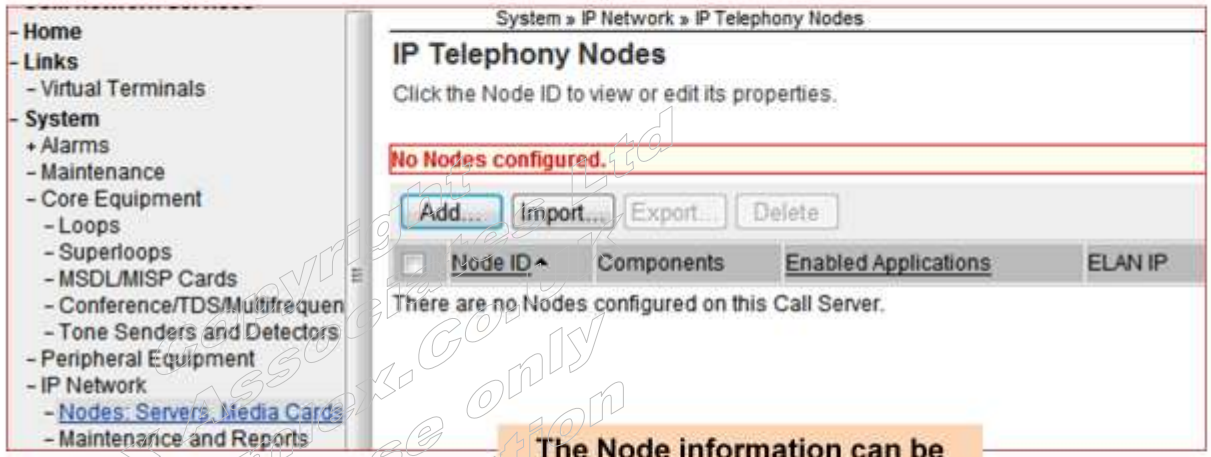
_____

IP Telephony Node

Node information in previous releases was imported from the Leader Signalling server. Since release 6 we do not add the same information when we build the Linux base so Nodes need to be defined manually or imported.

Information can be imported from an existing .xml file or another Node already in service and then edited to suit the new application.

To create a node from scratch click on the **ADD** button.



The Node information can be added manually or Imported from another existing Node or a node that has been exported to an xml file.

Amlex Associates Ltd Copyright www.Amlex.Co.Uk Personal use only Not for distribution

133

Notes

_____

_____

_____

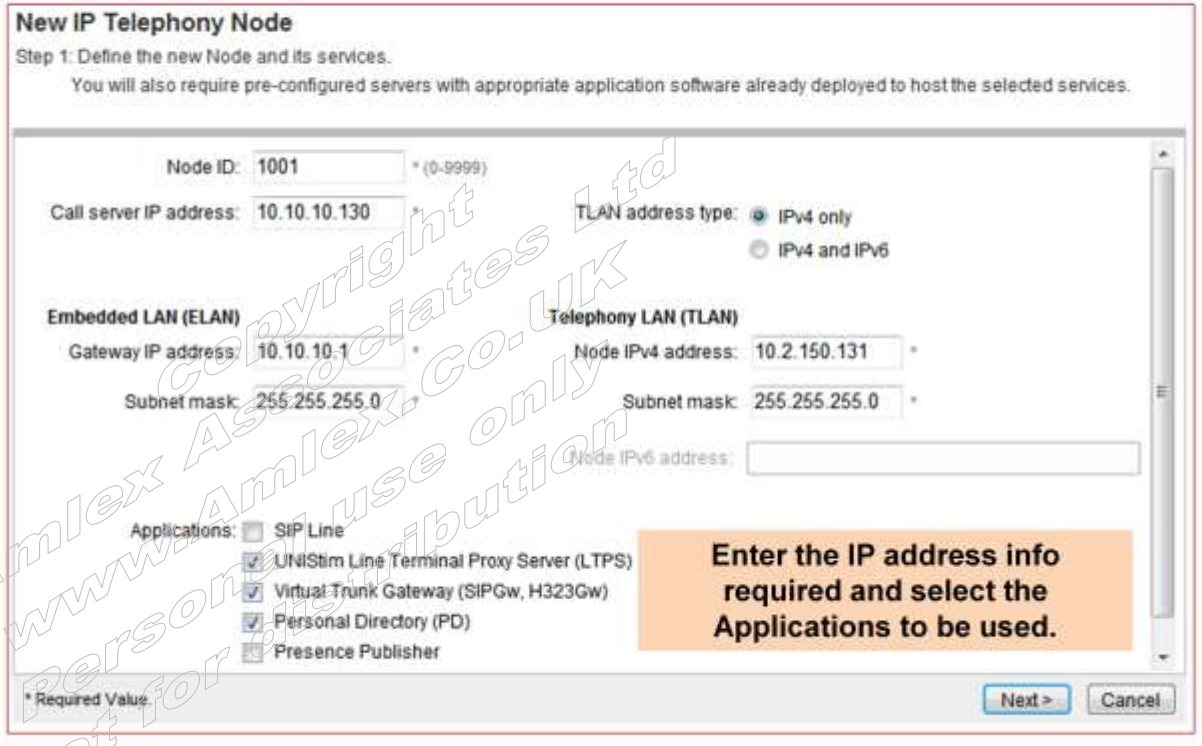
_____

Copyright Amlex Associates Ltd

Selecting Applications

On this page you need to add some basic address information, the Node ID number and the applications you wish to run within the Node.

Note that as this is a CoRes server SIP Line and Presence Publisher are showing as available to use. For now we will just add the UniStim TPS , Virtual Trunk Gateway and Personal Directory.


New IP Telephony Node
Step 1: Define the new Node and its services.
You will also require pre-configured servers with appropriate application software already deployed to host the selected services.
Node ID: 1001 * (0-9999)
Call server IP address: 10.10.10.130 *
TLAN address type: IPv4 only
IPv4 and IPv6
Embedded LAN (ELAN)
Gateway IP address: 10.10.10.1 *
Subnet mask: 255.255.255.0 *
Telephony LAN (TLAN)
Node IPv4 address: 10.2.150.131 *
Subnet mask: 255.255.255.0 *
Node IPv6 address:
Applications:
SIP Line
UNIStim Line Terminal Proxy Server (LTPS)
Virtual Trunk Gateway (SIPGw, H323Gw)
Personal Directory (PD)
Presence Publisher
Enter the IP address info required and select the Applications to be used.
* Required Value.
Next >
Cancel

134

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

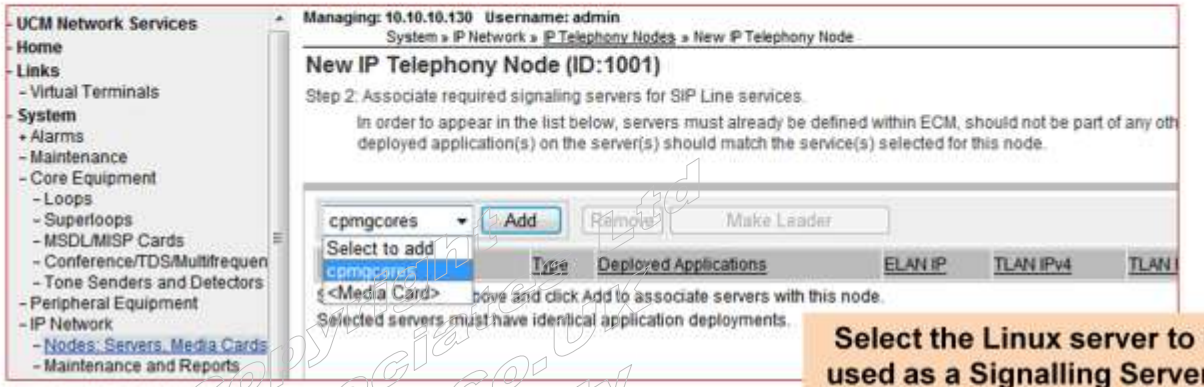
Add Server & Make Leader

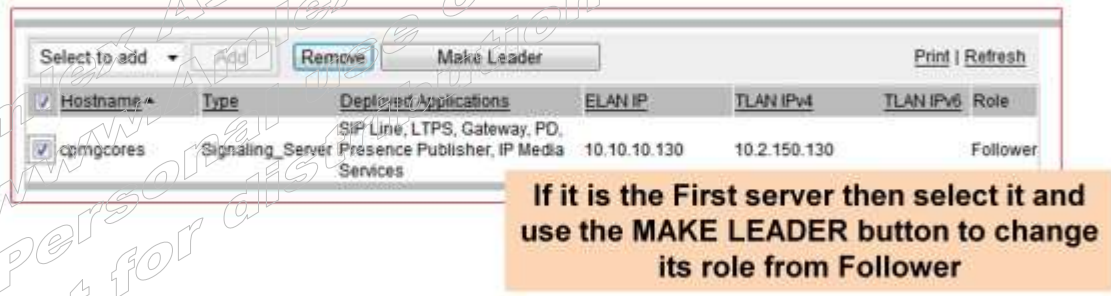
Similar to the pre-deployment we did earlier, we need to add the Signalling servers that will be used in the Node.

To do this click on the drop down menu **SELECT TO ADD** which will display all of the available servers which can be used.

If its the first or only server in the Node then it needs to be designated as the Leader by selecting it (Tick Box) and clicking the **MAKE LEADER** button.

Remember each Node must have a Leader signalling server to hold the Node IP address.


UCM Network Services
Home
Links
Virtual Terminals
System
Alarms
Maintenance
Core Equipment
Loops
Superloops
MSDL/MISP Cards
Conference/TDS/Multifrequen
Tone Senders and Detectors
Peripheral Equipment
IP Network
Nodes: Servers, Media Cards
Maintenance and Reports
Managing: 10.10.10.130 Username: admin
System » IP Network » IP Telephony Nodes » New IP Telephony Node
New IP Telephony Node (ID:1001)
Step 2: Associate required signaling servers for SIP Line services.
In order to appear in the list below, servers must already be defined within ECM, should not be part of any oth
deployed application(s) on the server(s) should match the service(s) selected for this node.
cpmgcores
Add
Remove
Make Leader
Select to add
cpmgcores
<Media Card>
Type
Deployed Applications
ELAN IP
TLAN IPv4
TLAN
bove and click Add to associate servers with this node.
Selected servers must have identical application deployments.
Select the Linux server to be used as a Signalling Server in the Node and ADD



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

135

Notes

_____

_____

_____

_____

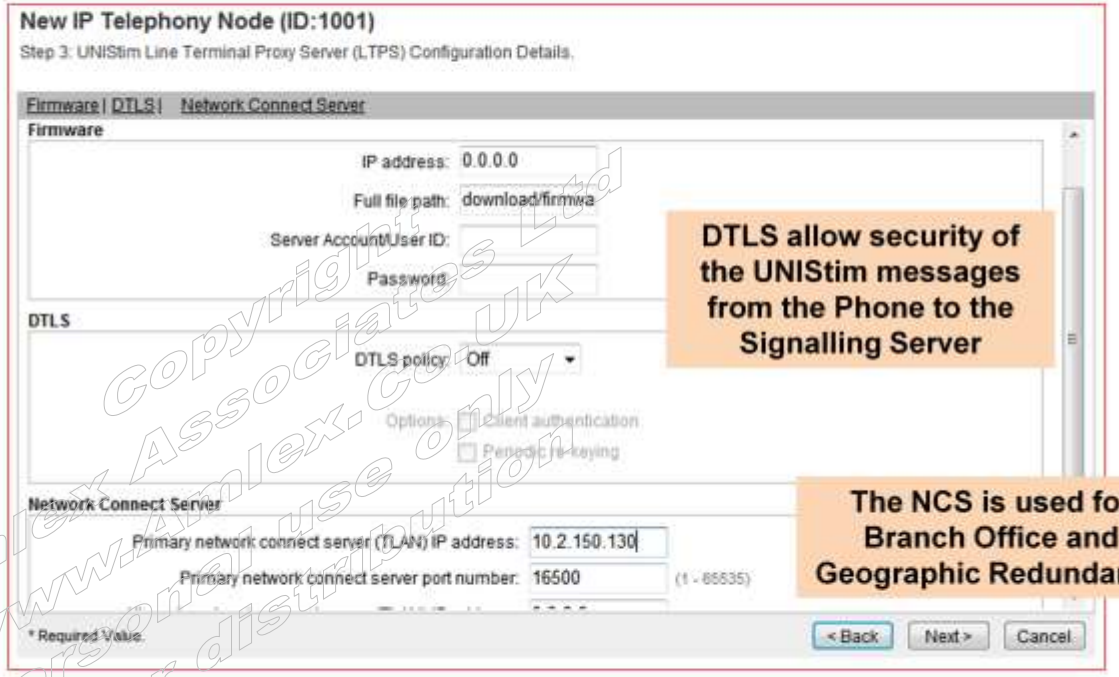
Firmware, DTLS & NCS

On this screen you can enter the IP address of an alternate Firmware server and also select if Datagram Transport Layer Security (DTLS – Security of Unistim to LTPS) is to be used and if so how e.g. Best Efforts or Always.

Again at this point we will ignore these options.

However the third option is the Network Connect Server (NCS) and we will need to add the IP address that will be used here. NCS is used for:-

Geographic Redundancy
Branch Office
Network Virtual Office.


New IP Telephony Node (ID:1001)
Step 3: UNIStim Line Terminal Proxy Server (LTPS) Configuration Details.
Firmware | DTLS | Network Connect Server
Firmware
IP address: 0.0.0.0
Full file path: download/firmwa
Server Account/User ID:
Password
DTLS
DTLS policy: Off
Options: Client authentication
Periodic re-keying
Network Connect Server
Primary network connect server (TLAN) IP address: 10.2.150.130
Primary network connect server port number: 16500 (1 - 65535)
* Required Value.
< Back
Next >
Cancel
DTLS allow security of the UNIStim messages from the Phone to the Signalling Server
The NCS is used for Branch Office and Geographic Redundancy

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

136

Notes

_____

_____

_____

_____

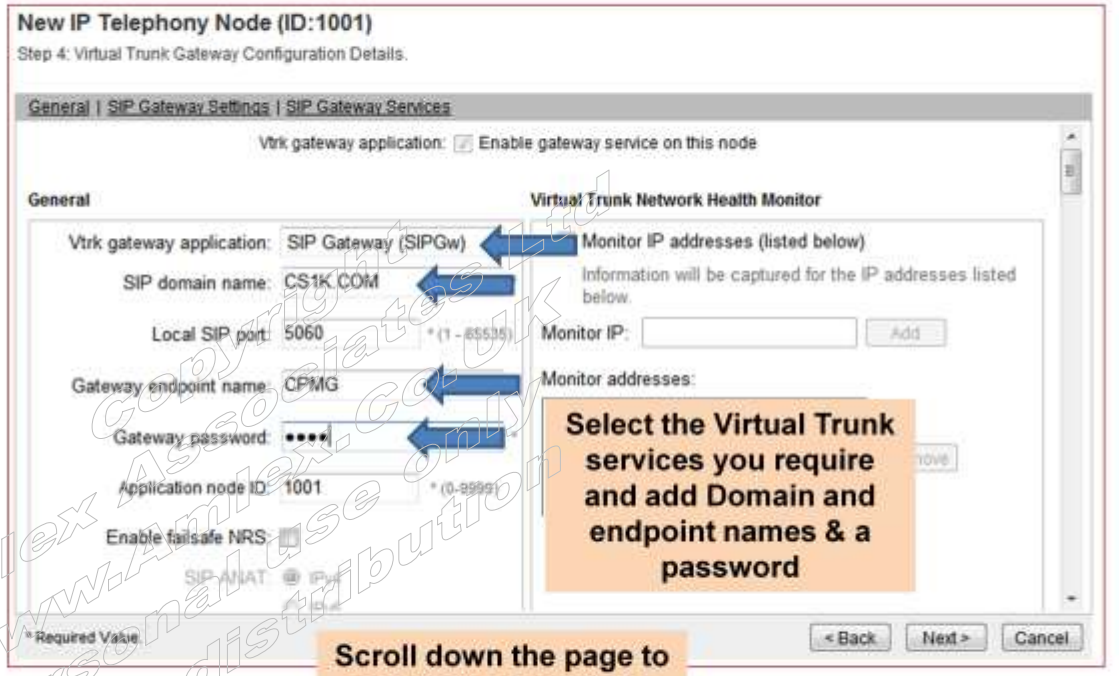
VTRK Signalling Gateway

Setting up the Virtual Trunk Signalling Gateway is the largest area of configuration and you need to ensure you have completed all mandatory fields before moving on.

The links at the top of the dialog (arrowed) can be used to move to different parts of the screen.

On this initial display we select which signalling we are supporting SIP and/or H.323. We also add the SIP Domain name and the endpoint names for the gateways. Ideally keep these the same as each other as shown here.

The Virtual Trunk Network Health Monitor is a mechanism to monitor an IP address (possibly a Router) and check it gets a response. Should the address stop responding the system will shut down the Virtual D-Channels for the Virtual Trunks.


New IP Telephony Node (ID:1001)
Step 4: Virtual Trunk Gateway Configuration Details.
General | SIP Gateway Settings | SIP Gateway Services
Vtrk gateway application: Enable gateway service on this node
General
Virtual Trunk Network Health Monitor
Vtrk gateway application: SIP Gateway (SIPGw)
SIP domain name: CS1K.COM
Local SIP port: 5060
Gateway endpoint name: CPMG
Gateway password: ••••
Application node ID: 1001
Enable failsafe NRS
Monitor IP addresses (listed below)
Information will be captured for the IP addresses listed below.
Monitor IP:
Add
Monitor addresses:
Select the Virtual Trunk services you require and add Domain and endpoint names & a password
* Required Value
< Back
Next >
Cancel
Scroll down the page to complete all sections

Amlex Associates Ltd www.Amlex.co.uk Copyright Personal use only Not for distribution

137

Notes

_____

_____

_____

_____

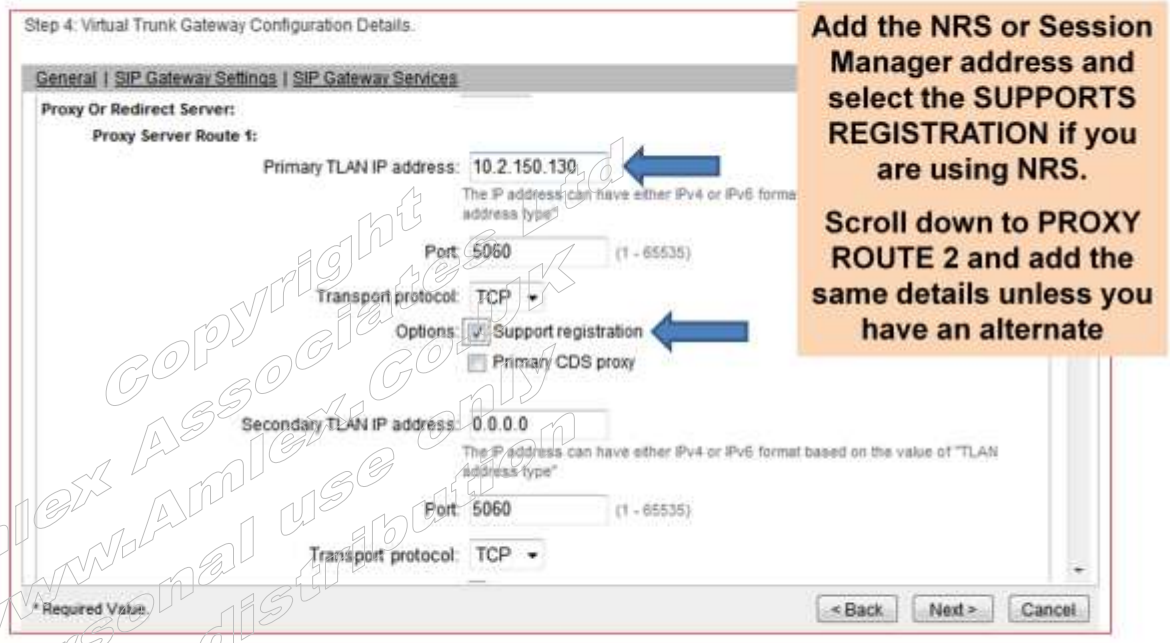
SIP Gateway

The SIP gateway screen is used to define where the SIP redirect or Proxy Server is located for the system. In CS1K terms this is the Network Routing Service (NRS) but in an Aura system implementation this would be the SIP entity address of the Session Manager.. Both the Primary and Secondary can be defined here allowing for redundancy.

Remember to tick the boxes for Registration and CDS so the gateway will register to the NRS.

The Transport Protocol is TCP by default for SIP.

Make the SIP Route 2 address the same as the Primary as the system will not allow it to be left blank.


Step 4: Virtual Trunk Gateway Configuration Details
General | SIP Gateway Settings | SIP Gateway Services
Proxy Or Redirect Server:
Proxy Server Route 1:
Primary TLAN IP address: 10.2.150.130
The IP address can have either IPv4 or IPv6 forma
address type"
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Primary CDS proxy
Secondary TLAN IP address: 0.0.0.0
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"
Port: 5060 (1 - 65535)
Transport protocol: TCP
* Required Value
< Back
Next >
Cancel
Add the NRS or Session Manager address and select the SUPPORTS REGISTRATION if you are using NRS.
Scroll down to PROXY ROUTE 2 and add the same details unless you have an alternate

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

138

Notes

_____

_____

_____

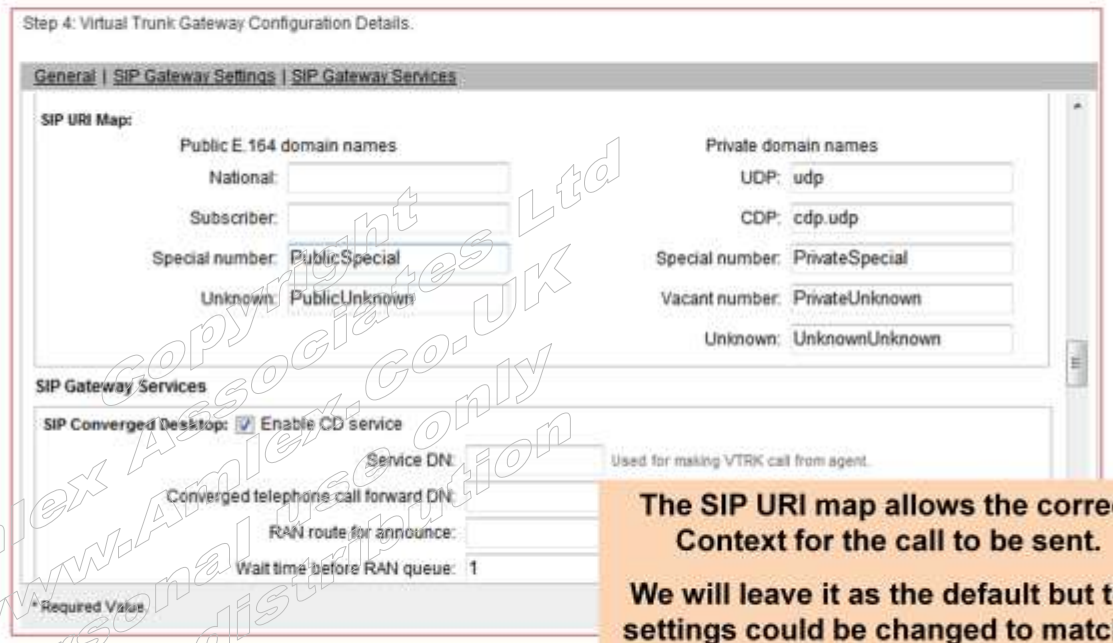
_____

SIP URI Map

The SIP Universal Resource Identifier is the mechanism that defines the context of each SIP call. SIP being Domain based needs this to ensure unique identities are achieved.

The Context is sent with each SIP request and is made up from the URI map shown and the SIP Domain configured earlier.

We will leave these as the Default CDP and UDP settings for now and discuss the implications of these settings later in the course.



The SIP URI map allows the correct Context for the call to be sent.

We will leave it as the default but the settings could be changed to match a customers Domains.

Copyright Amlex Associates Ltd www.Amlex.co.UK Personal use only Not for distribution

139

Notes

_____

_____

_____

_____

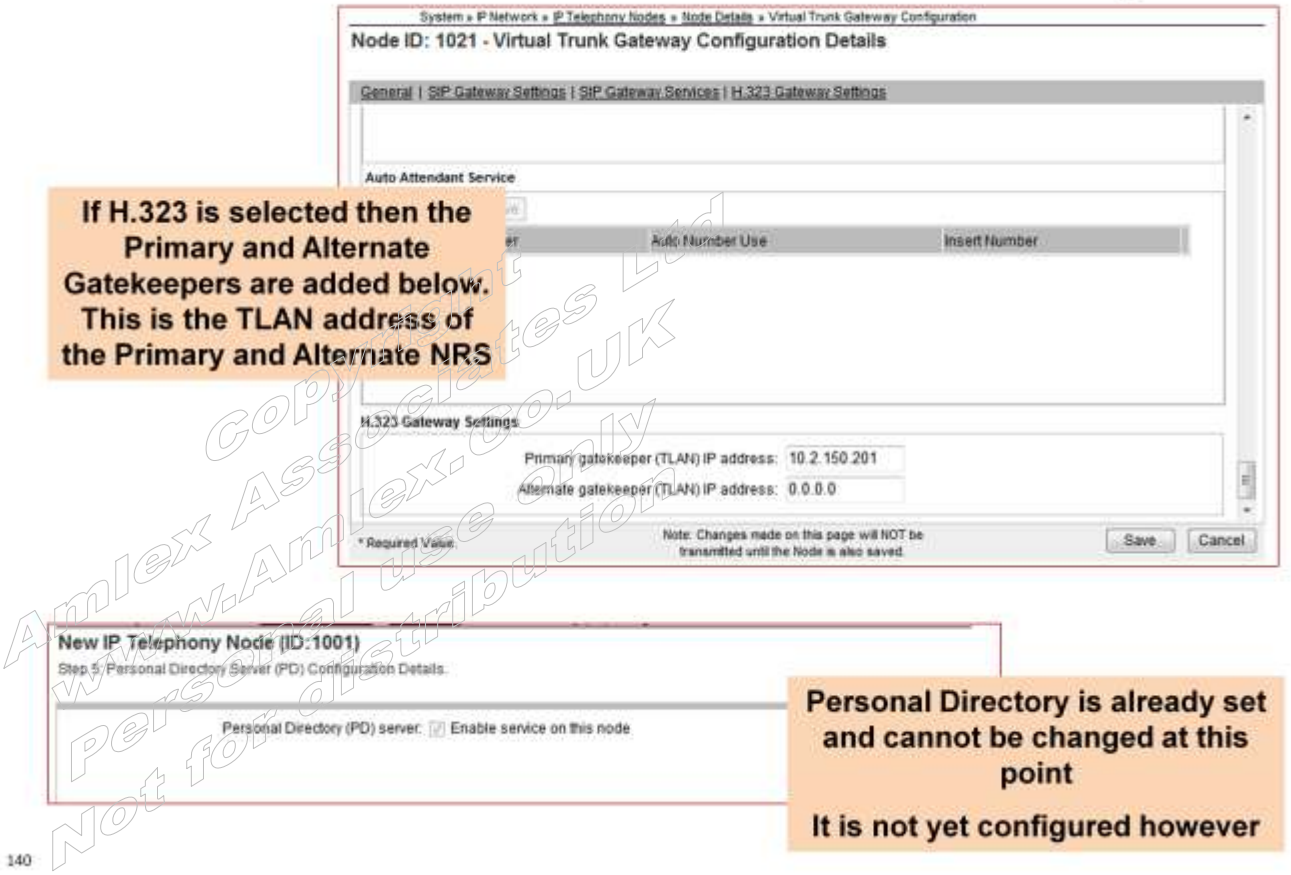
H.323 & Personal Directory

On this screen we are adding the H323 information which again will allow the Signalling Gateway to register and setup Virtual Trunk calls.

The Primary and Secondary Gatekeeper are used to route H.323 calls and correspond to the to the Primary and Alternate NRS respectively. Even in an Aura implementation this will be the case as Session Manager does not handle H.323 Routing.

Personal Directory was requested on the initial screen and thus this is just a confirmation screen.

Remember that the PD is still not configured for use by IP sets so this will be done later on the dialogue just confirms it is available on the node.


System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration
Node ID: 1021 - Virtual Trunk Gateway Configuration Details
General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings
Auto Attendant Service
Auto Number Use
Insert Number
If H.323 is selected then the Primary and Alternate Gatekeepers are added below. This is the TLAN address of the Primary and Alternate NRS
H.323 Gateway Settings
Primary gatekeeper (TLAN) IP address: 10.2.150.201
Alternate gatekeeper (TLAN) IP address: 0.0.0.0
* Required Value
Note: Changes made on this page will NOT be transmitted until the Node is also saved.
Save
Cancel
New IP Telephony Node (ID:1001)
Step 5: Personal Directory Server (PD) Configuration Details
Personal Directory (PD) server: Enable service on this node
Personal Directory is already set and cannot be changed at this point
It is not yet configured however
140

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Save & Transfer

The final screen here shows a summary of what has been configured and gives the option to save or discard or change the configuration.

Clicking the **FINISH** button will save the configuration and take you to the next screen (Below) where you can transfer the information to all of the servers in the Node.

If you are happy with the configuration created, click on the **TRANSFER NOW** button. If you need to do further editing of the Node Click on **SHOW NODES.**

New IP Telephony Node (ID:1001)
Step 6: Confirm new Node details.
Review the new Node definition and click Finish to commit.
Node ID: 1001
Node IPv4 address: 10.2.150.131
Node IPv6 address:
Domain: CS1K.COM
Application(s): LTPS, PD, Gateway (SIPGw)
Servers: cpmgcores
Save the new Node by clicking Finish below. Configuration details will be transmitted to associated servers, which will require a reboot.
In order to make this new node and the IP phones associated with it completely functional, you must create a route for the associated customer.
Managing: 10.10.10.130 Username: admin
System » IP Network » IP Telephony Nodes » Node Saved
Node Saved
Node ID: 1001 has been saved on the call server.
The new configuration must also be transferred to associated servers and media cards.
Transfer Now...
You will be given an option to select individual servers, or transfer to all.
Show Nodes
You may initiate a transfer manually at a later time.

Amlex Associates Ltd
www.Amlex.co.UK
Copyright
Personal use only
Not for distribution

141

Notes

_____

_____

_____

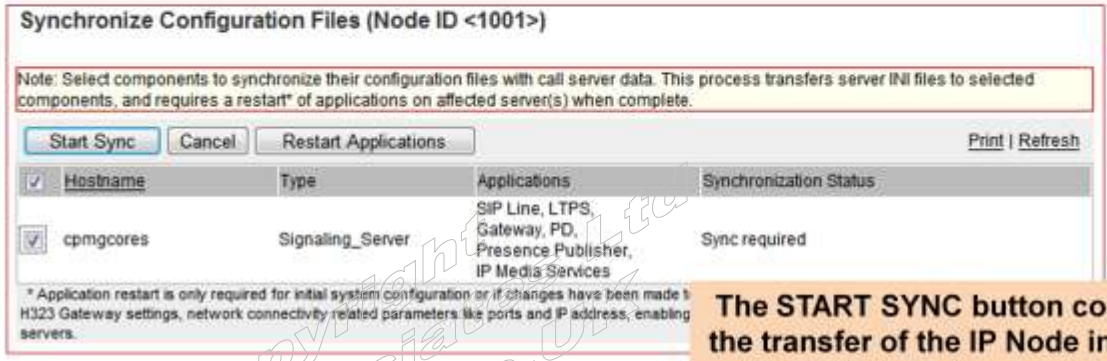
_____

Synchronise Node

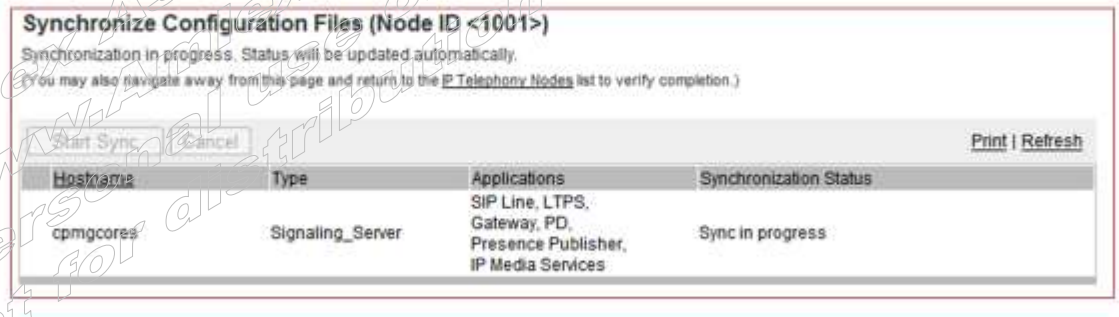
Having clicked the **TRANSFER NOW** button you are presented with the dialogue shown where you can select the relevant servers and then send the configuration to them using the **START SYNC** button.

The lower display shows the on screen feedback as the synchronise takes place.

The status will show Synchronised when it is complete.


Synchronize Configuration Files (Node ID <1001>)
Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.
Start Sync
Cancel
Restart Applications
Print | Refresh
Hostname
Type
Applications
Synchronization Status
cpmgcores
Signaling_Server
SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services
Sync required
* Application restart is only required for initial system configuration or if changes have been made t
H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling
servers.

The START SYNC button commences the transfer of the IP Node information to each of the Node components


Synchronize Configuration Files (Node ID <1001>)
Synchronization in progress. Status will be updated automatically.
(You may also navigate away from this page and return to the IP Telephony Nodes list to verify completion.)
Start Sync
Cancel
Print | Refresh
Hostname
Type
Applications
Synchronization Status
cpmgcores
Signaling_Server
SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services
Sync in progress

142

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

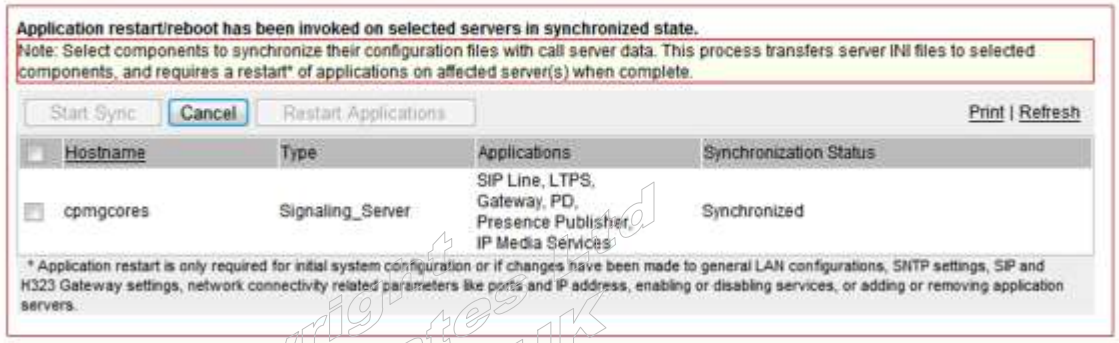
Restart IP Node

If this is the first time the Node had been synchronised or if some major change has been made it is necessary to Restart the IP Node software.

This is done by selecting the servers again via the tick boxes and clicking the **RESTART APPLICATIONS** button.

An easy way to check when the IP Node is up and operational is to Ping the Node IP Address as shown in the lower screenshot.

Until the Node IP address responds you will not be able to register IP sets so its a quick and easy check to make.


Application restart/reboot has been invoked on selected servers in synchronized state.
Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart* of applications on affected server(s) when complete.
Start Sync
Cancel
Restart Applications
Print | Refresh
Hostname
Type
Applications
Synchronization Status
cpmgcores
Signaling_Server
SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services
Synchronized
* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

When the Synchronise is complete if this is the initial transfer or if the Node has been edited significantly it is necessary to click RESTART APPLICATIONS to ensure the software is running the latest configuration.

```
Ping statistics for 10.2.150.130:
    Packets: Sent = 22, Received = 19, Lost = 3 (13% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\Phil>ping 10.2.150.131

Pinging 10.2.150.131 with 32 bytes of data:
Reply from 10.2.150.131: bytes=32 time<1ms TTL=64
Reply from 10.2.150.131: bytes=32 time<1ms TTL=64
Reply from 10.2.150.131: bytes=32 time<1ms TTL=64
Reply from 10.2.150.131: bytes=32 time<1ms TTL=64

Ping statistics for 10.2.150.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Phil>
```

143

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

There are a few things you need to have on hand before you configure sets on the system. The main difference between a Digital set and an IP set is the IP configuration although in reality this isn't needed for the actual configuration on the system but when the set is registered.

Two things you must have for the IP set are a Virtual TN and a Bandwidth Zone.

To see what Virtual TN's are available on the system you can list the Superloops in LD 97, List Unused Cards - LUC in LD 20 or List Unused Voice Units - LUVU in LD 20. Zones can be listed in LD 117 - PRT INTRA.

To find available DN's try List Unused DN in LD 20 – LUDN .

Once you have a set configured with all the buttons and features required you can copy it and create multiple copies

```
REQ: cpy 4
TYPE: 1140
CFTN 252 0 0 0   - From TN
DES  1140
SFMT auto          - Auto assign TN & DN
TN   252 0 5 0     - Start TN
DN   1750          - Start DN

NEW 1140   TN  252 0 05 00   DN  1750
NEW 1140   TN  252 0 05 01   DN  1751
NEW 1140   TN  252 0 05 02   DN  1752
NEW 1140   TN  252 0 05 03   DN  1753
```

144

12. Configuring Sets

- IP Set
  - Set Type
    - 1140 etc.
  - Virtual TN
    - Any unused VTN
  - Bandwidth Zone
    - Main Office B/W Zone
  - DN
    - To apply to Keys
  - Features etc.
    - Class of Service
    - NCOS etc
  - IP Configuration
    - IP Address

- Digital Set
  - Set Type
    - 39XX etc
  - TN of Card
    - Which Shelf or Media Gateway is the card installed and which unit.
  - DN
    - To Apply to Keys
  - Features etc.
    - Class of Service
    - NCOS etc

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Key Options (1140)

On sets with multiple keys there are many options which maybe added to make the set as easy to use as possible. The figure shows the options displayed on the Basic Client Configuration tool for an IP 1140 set.

One thing to be aware of is the interaction between some Keys. When trying to apply a key or to make a change the system will respond with an error (SCH Code) because of a conflict with another existing set, say a DN already used else where .

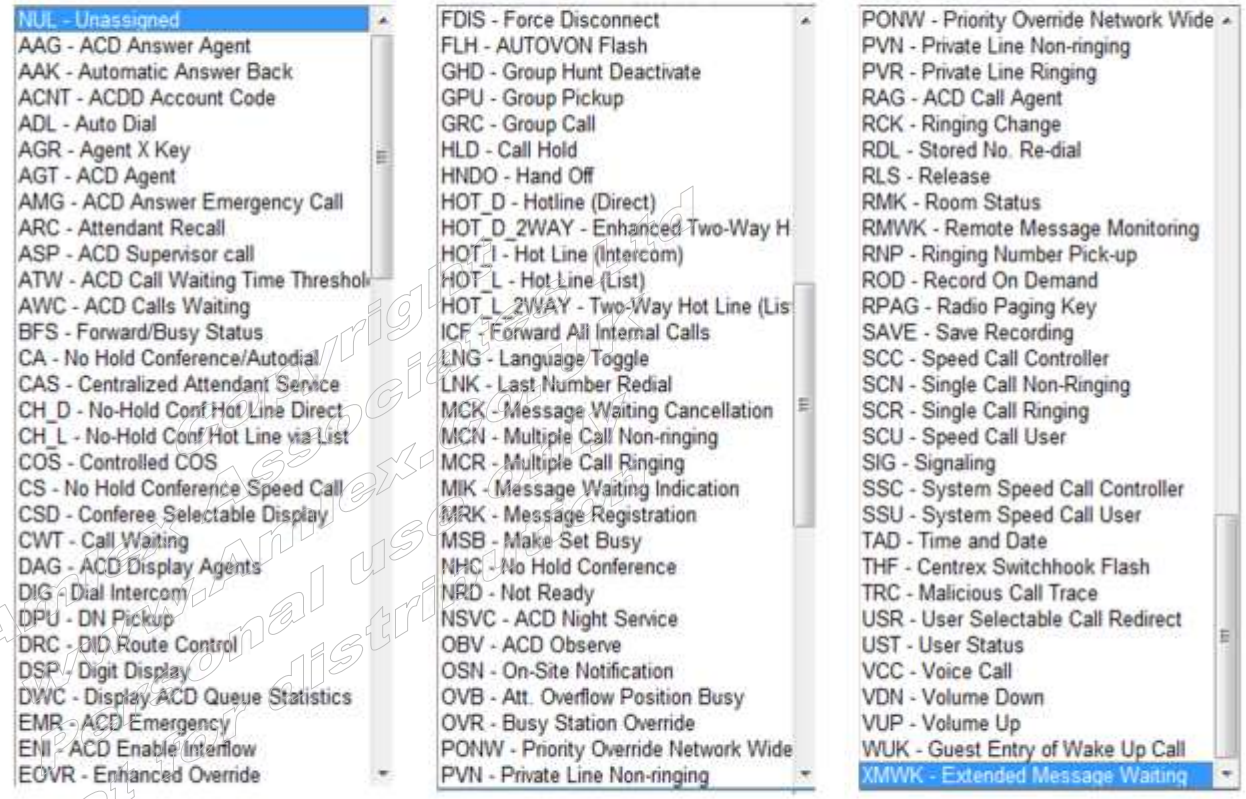
Sets are configured and edited in LD 20 and remember the prompts here have a ":" so you can get help if you cant remember what to input.

To create a set NEW

To delete a set OUT

To edit a set CHG
Answer yes to the prompt ECHG to enter particular items and their changes.

To change an IP set type CHGTYP


NUL - Unassigned
AAG - ACD Answer Agent
AAK - Automatic Answer Back
ACNT - ACDD Account Code
ADL - Auto Dial
AGR - Agent X Key
AGT - ACD Agent
AMG - ACD Answer Emergency Call
ARC - Attendant Recall
ASP - ACD Supervisor call
ATW - ACD Call Waiting Time Threshol
AWC - ACD Calls Waiting
BFS - Forward/Busy Status
CA - No Hold Conference/Autodial
CAS - Centralized Attendant Service
CH_D - No-Hold Conf Hot Line Direct
CH_L - No-Hold Conf Hot Line via List
COS - Controlled COS
CS - No Hold Conference Speed Call
CSD - Conferee Selectable Display
CWT - Call Waiting
DAG - ACD Display Agents
DIG - Dial Intercom
DPU - DN Pickup
DRC - DID Route Control
DSP - Digit Display
DWC - Display ACD Queue Statistics
EMR - ACD Emergency
ENI - ACD Enable Interflow
EOVR - Enhanced Override
FDIS - Force Disconnect
FLH - AUTOVON Flash
GHD - Group Hunt Deactivate
GPU - Group Pickup
GRC - Group Call
HLD - Call Hold
HNDO - Hand Off
HOT_D - Hotline (Direct)
HOT_D_2WAY - Enhanced Two-Way H
HOT_I - Hot Line (Intercom)
HOT_L - Hot Line (List)
HOT_L_2WAY - Two-Way Hot Line (Lis
ICF - Forward All Internal Calls
LNG - Language Toggle
LNK - Last Number Redial
MCK - Message Waiting Cancellation
MCN - Multiple Call Non-ringing
MCR - Multiple Call Ringing
MIK - Message Waiting Indication
MRK - Message Registration
MSB - Make Set Busy
NHC - No Hold Conference
NRD - Not Ready
NSVC - ACD Night Service
OBV - ACD Observe
OSN - On-Site Notification
OVB - Att. Overflow Position Busy
OVR - Busy Station Override
PONW - Priority Override Network Wide
PVN - Private Line Non-ringing
PONW - Priority Override Network Wide
PVN - Private Line Non-ringing
PVR - Private Line Ringing
RAG - ACD Call Agent
RCK - Ringing Change
RDL - Stored No. Re-dial
RLS - Release
RMK - Room Status
RMWK - Remote Message Monitoring
RNP - Ringing Number Pick-up
ROD - Record On Demand
RPAG - Radio Paging Key
SAVE - Save Recording
SCC - Speed Call Controller
SCN - Single Call Non-Ringing
SCR - Single Call Ringing
SCU - Speed Call User
SIG - Signaling
SSC - System Speed Call Controller
SSU - System Speed Call User
TAD - Time and Date
THF - Centrex Switchhook Flash
TRC - Malicious Call Trace
USR - User Selectable Call Redirect
UST - User Status
VCC - Voice Call
VDN - Volume Down
VUP - Volume Up
WUK - Guest Entry of Wake Up Call
XMWK - Extended Message Waiting

145

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Configuring Sets - Overlays

Phone Sets can be configured in LD 10 (Analogue), LD 11 (Digital & IP) or LD 20 (Either). Below is a configuration for an analogue (500) set, where the FALC (Flexible Analogue Card) is located in Media Gateway 0 0 card slot 2

```
REQ NEW
TYPE:
TYPE 500        Analogue set on FALC
TN   0 0 2 0
CDEN
DES  500
CUST 0
ERL
WRLS NO
DN   1200
MIX
  MARP ON TN 000 0 02 00
  MARP
  CPND
  VMB
```

ld 20

```
REQ: new
TYPE: 1140          SET Type
TN   252 0 0 10     Virtual TN
DES  1140
CUST 0
NUID
NHTN
KEM
ZONE 1              Bandwidth Zone
ERL
ECL
FDN
TGAR 0
LDN
NCOS
RNPG
SSU
SGRP
SFLT
CAC_MFC
```

```
CLS
HUNT
SCI
PLEV
DANI
AST
IAPG
MLWU_LANG
MLNG
DNDR
KEY 0 scr 1000      DN for Key 0
 MARP
 CPND
 VMB
KEY 1 scr 1100      DN for Key 1
 MARP
 CPND
 VMB
KEY

MGMT001 TNB NEW TYPE:1140 TN:252 0 0
    10
```

146

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

IP sets need configuration so they will register to the correct call server. This can be done using the DHCP server and sending a full string of configuration parameters to the set. It can also be done manually by accessing the configuration menu.

On the 1100 series phones this can be done by pressing twice on the services key which will present a further menu. Select Network configuration from this menu and use the navigation keys to select the parameters to change using the central select key.

On the 200X sets press the 4 keys below the display when the set restarts and “AVAYA” is displayed. This will then allow you to step through the configuration parameters.

To reset a phone either power it down and back up or use the following key sequence:-

MUTE UP DOWN UP DOWN UP MUTE 9 RELEASE.

S1 = Node IP Address of the system
S1 Port = 4100
S1 Action = 1
S1 Retry Count = Registration attempts

IP Set Configuration

S1 & S2 should contain the NODE IP Address of the systems to which the phones can register
Press Services key twice to Access configuration Menu
As set starts up press all 4 keys in succession when AVAYA is displayed

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

147

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Many times the requirement is to change a number or feature on a set or remove it completely.

To Change a feature you can invoke easy change as shown here that allows you to change just the specific item rather than step through every prompt. Here we are changing Key 0 (Primary DN) to an SCR Single Call Ring with the DN 1111 and also adding a name to it.

Also shown are the options to COPY an existing set configuration to a single new set or multiple sets. Note that the example shows the automatic option to increment the TN and DN for the new sets.

To completely remove a set use the OUT command at the REQ prompt as shown here. You will also need to input the Type and TN .

Configuring Sets

Changing Sets

- REQ CHG
- TYPE: - Set Type to change
- TYPE 1140
- TN 252 0 15 0 - TN
- ECHG yes - Easy Change
- ITEM key 0 scr 1111 - Item to change
- MARP
- CPND new - Add New name
- CPND_LANG
- NAME
- Phil Pattington
- XPLN
- DISPLAY_FMT
- VMB
- KEY
- ITEM

Copy Sets

- REQ: cpy 4
- TYPE: 1140
- CFTN 252 0 0 0 - From TN
- DES 1140
- SFMT auto - Auto assign TN & DN
- TN 252 0 5 0 - Start TN
- DN 1750 - Start DN

Removing Sets

- REQ: out - Remove set on TN
- TYPE: 1140
- TN 252 0 15 0

Amlex Copyright www.amlex.co.uk Personal use only Not for distribution

148

Notes

_____

_____

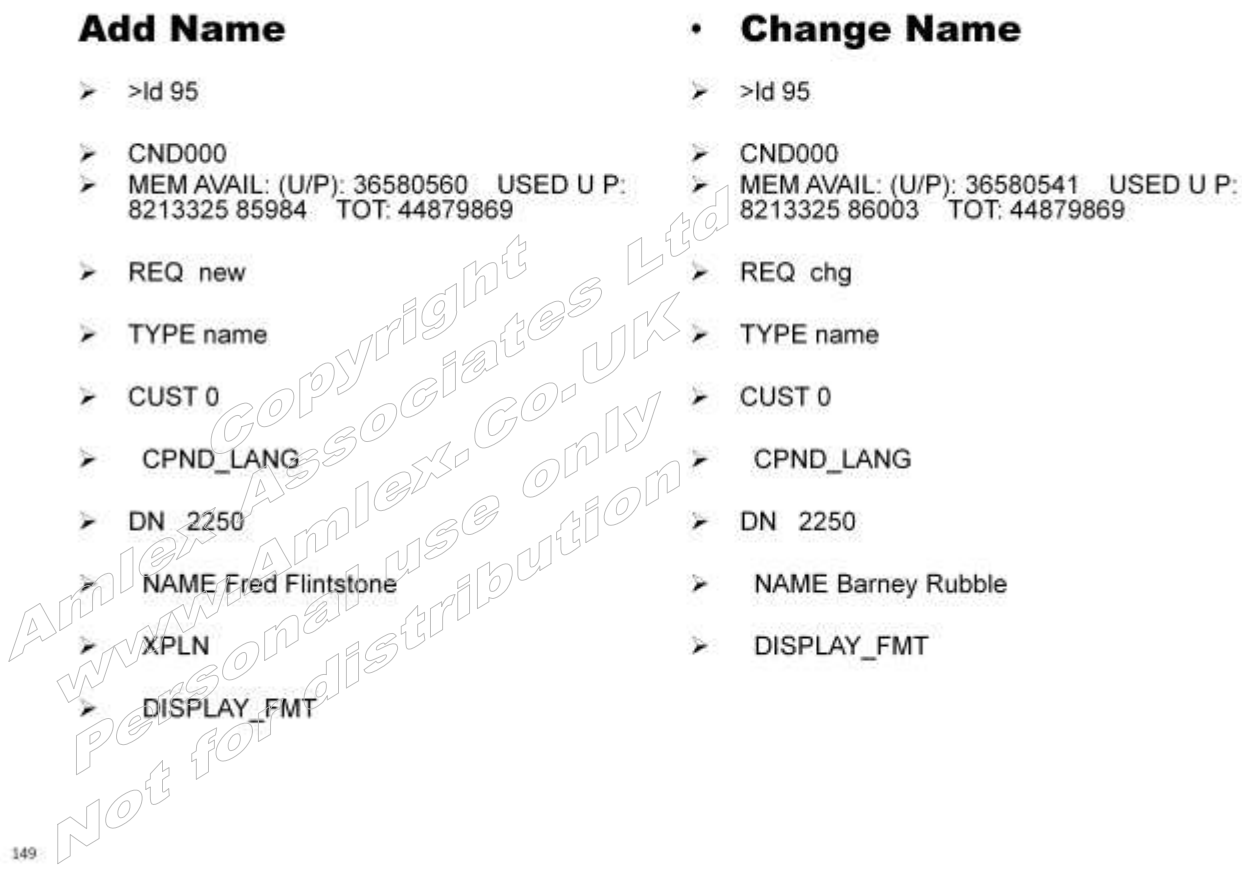
_____

_____

Add or Change Names on Set

A regular occurrence maybe the change of the Name associated with a set. Whilst this can be done in Overlay 20 by changing the set it can also be done in Overlay 95 as shown here.

Note that if a name is already associated with a DN you should use the CHG (Change) option rather than the NEW. Type is always NAME.



Copyright Amlex Associates Ltd www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Pickup Groups are used to allow users to “Pickup” calls to other handsets in the same Pickup Group.

The Ringing Pickup Group is defined as soon as the Prompt RNPG has a number defined against it. This is the Group number and can be added to other sets as required.

In addition the set picking up the calls will need the necessary Class of Service to enable the service.

Pickup Groups

- **When you make a phone TN's RNPG = " a Number", a Pickup Group is created with that number and the set is included in it.**

- **When you assign the RNPG number to another phone it also becomes a member of that Pickup Group.**

- >ld 20
- PT0000
- REQ: CHG
- TYPE: 500
- TN 0 0 2 10
- ECHG YES
- ITEM RNPG 10 - Pickup Group 10
- ITEM CLS PUA - Pickup Allowed
- ITEM CLS GPUA - Group Pickup
- ITEM

Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

150

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add Phones via Element Manager

Release 6 added the Basic Client Configurator (BCC) option to Element Manager and this is extended with Rel 7 in line with the end of life of Telephony Manager.

BCC allows for sets to be created through the web interface. By selecting the **PHONES** option in Element manager.

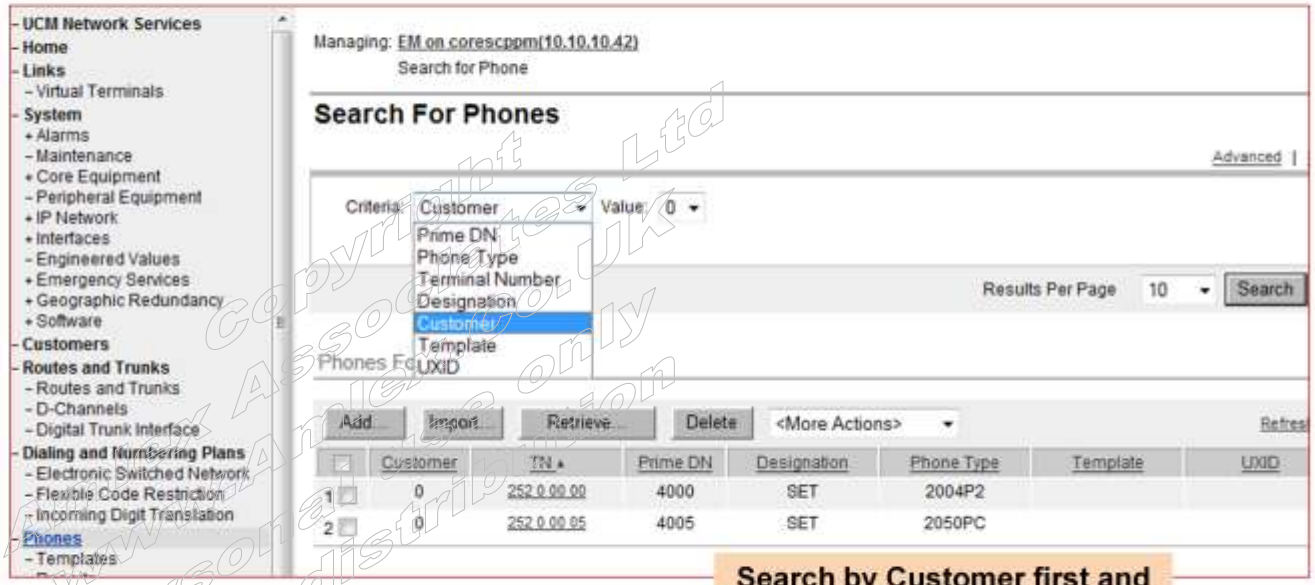
The search screen shown will be displayed. It is best to select search by **CUSTOMER 0** and click **SEARCH** to update the local cache. If this fails to display anything try clicking the **RETRIEVE** button and selecting the option **ALL PHONES AND RECONCILE** and then SUBMIT.

This should display any existing phones.

The **ADD, IMPORT, RETRIEVE, DELETE** and **MORE ACTIONS** in the lower part of the screen are used to create and edit phones.

The **IMPORT** option allows for the creation of sets from a CSV file and can be useful for bulk import of phones.

A Template may be created from a set using the **MORE ACTIONS** drop down menu.



Search by Customer first and use RETRIEVE button for All Sets & Reconcile

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

1S1

Notes

_____

_____

_____

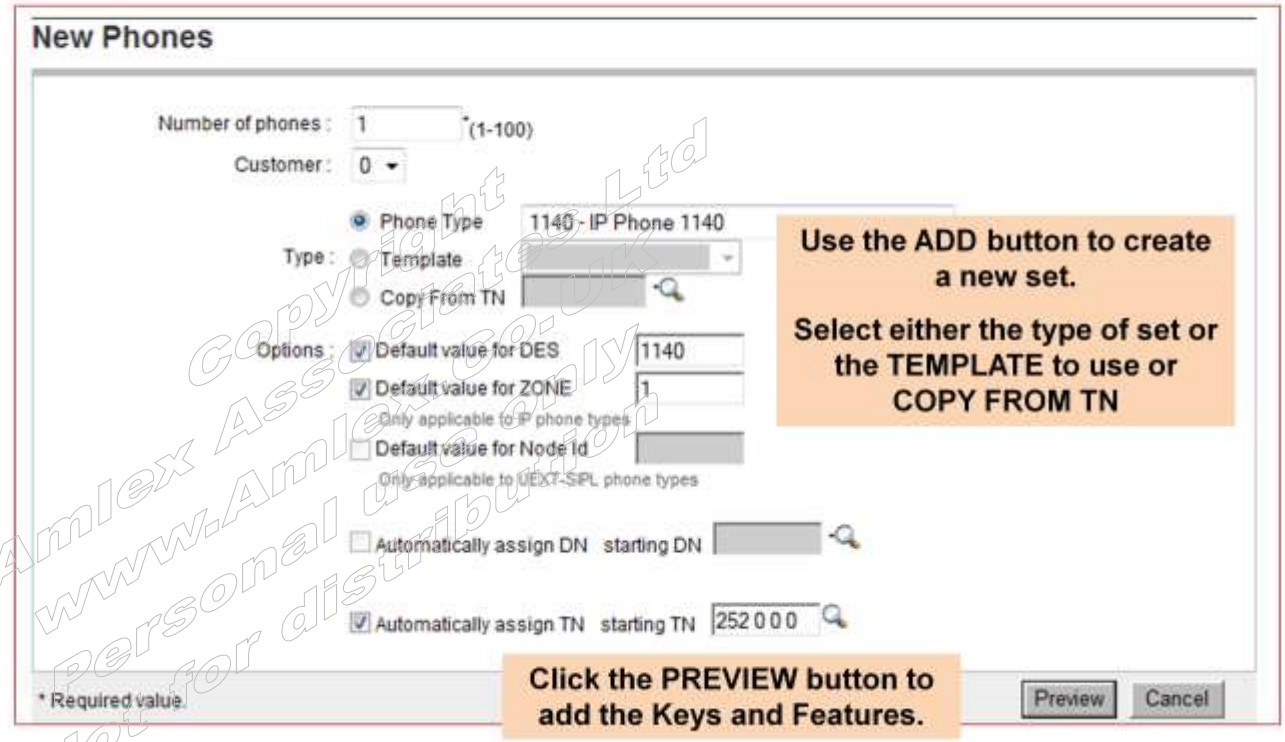
_____

Add New Sets

To add a new set use the **ADD** button which will display the screen shown here.

Select the options you require Type, Template etc and then click on the **PREVIEW** button to allow the system to check if the configuration is valid or not.

Sets can be copied from existing units or created using Templates. Adding as much information as possible at this point will speed the process.


New Phones
Number of phones : 1 (1-100)
Customer : 0
Type :
Phone Type 1140 - IP Phone 1140
Template
Copy From TN
Options :
Default value for DES 1140
Default value for ZONE 1
Only applicable to IP phone types
Default value for Node Id
Only applicable to UEXT-SPL phone types
Automatically assign DN starting DN
Automatically assign TN starting TN 252000
* Required value
Use the ADD button to create a new set.
Select either the type of set or the TEMPLATE to use or COPY FROM TN
Click the PREVIEW button to add the Keys and Features.
Preview
Cancel

Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

152

Notes

_____

_____

_____

_____

Select Features and Keys

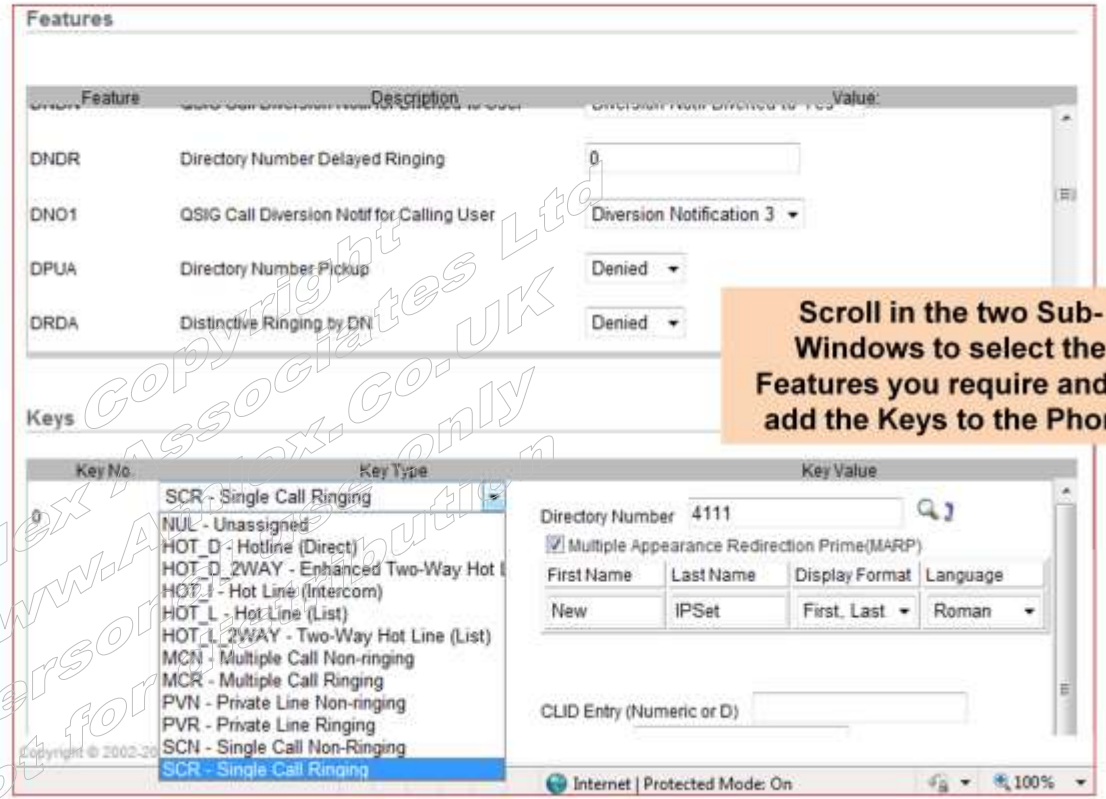
After using the **PREVIEW** button you will be presented with a screen which allows the selection of the Features and Keys required fro the set.

Many are presented as Drop down lists to speed the selection.

When complete use the **VALIDATE** button at the bottom of the page to check the configuration for errors.

If it completes the check okay then use the **FINISH** button to create the set on the system.

BCC although it looks similar to Telephony Manager (TM) is different in a significant respect and that is when it tries to create a set. TM is a batch system and changes are done offline with the updates being transmitted later. BCC tries to create the set as soon as you complete the configuration.



153

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

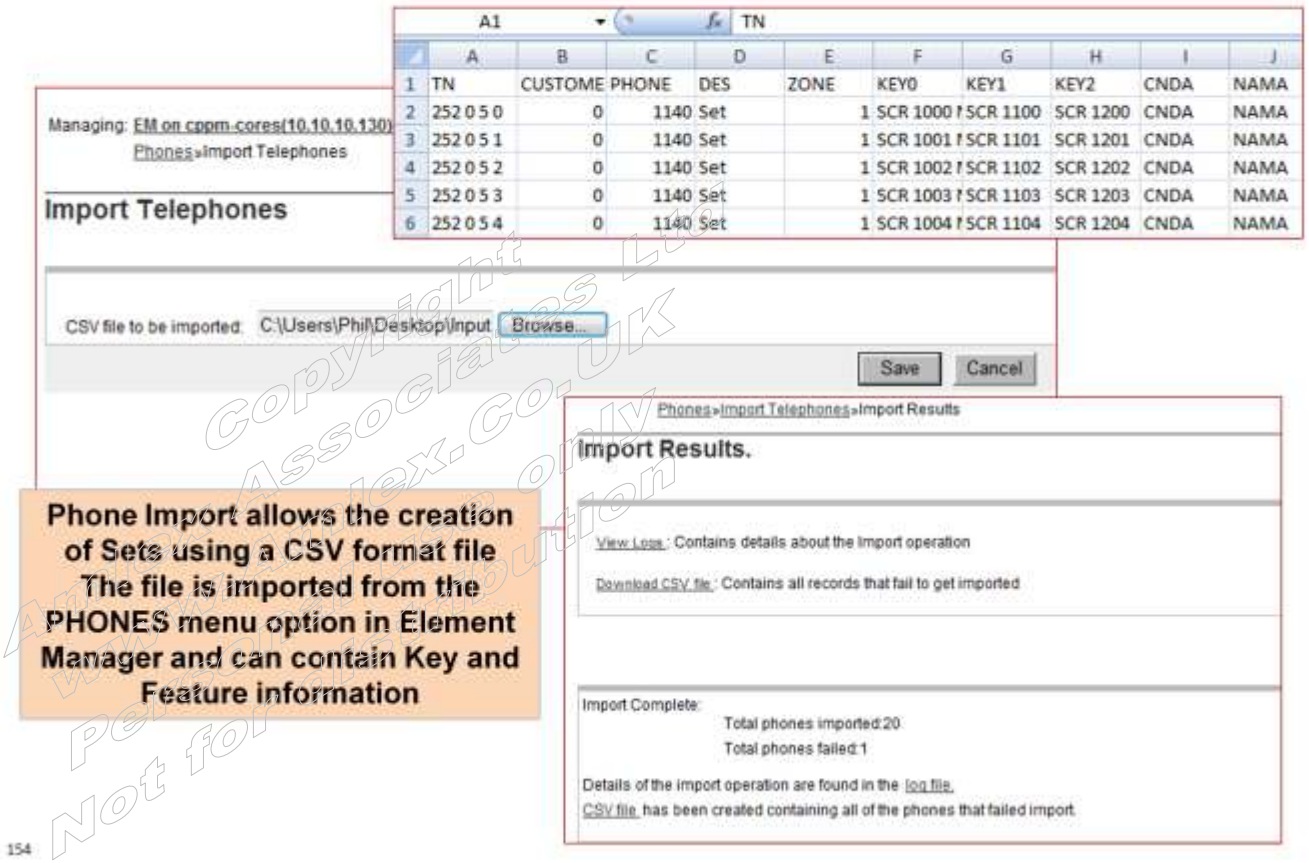
Phone Import

Using the Phone Import option can be a good way to create several phones on a system quickly.

The format of the CSV file used is flexible with only a few fields being mandatory. However it can be expanded to add Name information as well as detailed Feature assignment.

See the relevant NTP for the full scope of the CSV file format.

When sets are imported using the Import option a log file is generated and any failures listed enabling you to correct problems and re-import.


A1
TN
A B C D E F G H I J
1 TN CUSTOME PHONE DES ZONE KEY0 KEY1 KEY2 CNDA NAMA
2 252 0 5 0 0 1140 Set 1 SCR 1000 SCR 1100 SCR 1200 CNDA NAMA
3 252 0 5 1 0 1140 Set 1 SCR 1001 SCR 1101 SCR 1201 CNDA NAMA
4 252 0 5 2 0 1140 Set 1 SCR 1002 SCR 1102 SCR 1202 CNDA NAMA
5 252 0 5 3 0 1140 Set 1 SCR 1003 SCR 1103 SCR 1203 CNDA NAMA
6 252 0 5 4 0 1140 Set 1 SCR 1004 SCR 1104 SCR 1204 CNDA NAMA
Managing: EM on cppm-cores(10.10.10.130)
Phones»Import Telephones
Import Telephones
CSV file to be imported: C:\Users\Phil\Desktop\Input Browse...
Save Cancel
Phones»Import Telephones»Import Results
Import Results.
View Logs : Contains details about the Import operation
Download CSV file : Contains all records that fail to get imported
Import Complete:
Total phones imported:20
Total phones failed:1
Details of the import operation are found in the log file.
CSV file has been created containing all of the phones that failed import.
Phone Import allows the creation of Sets using a CSV format file The file is imported from the PHONES menu option in Element Manager and can contain Key and Feature information
154

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

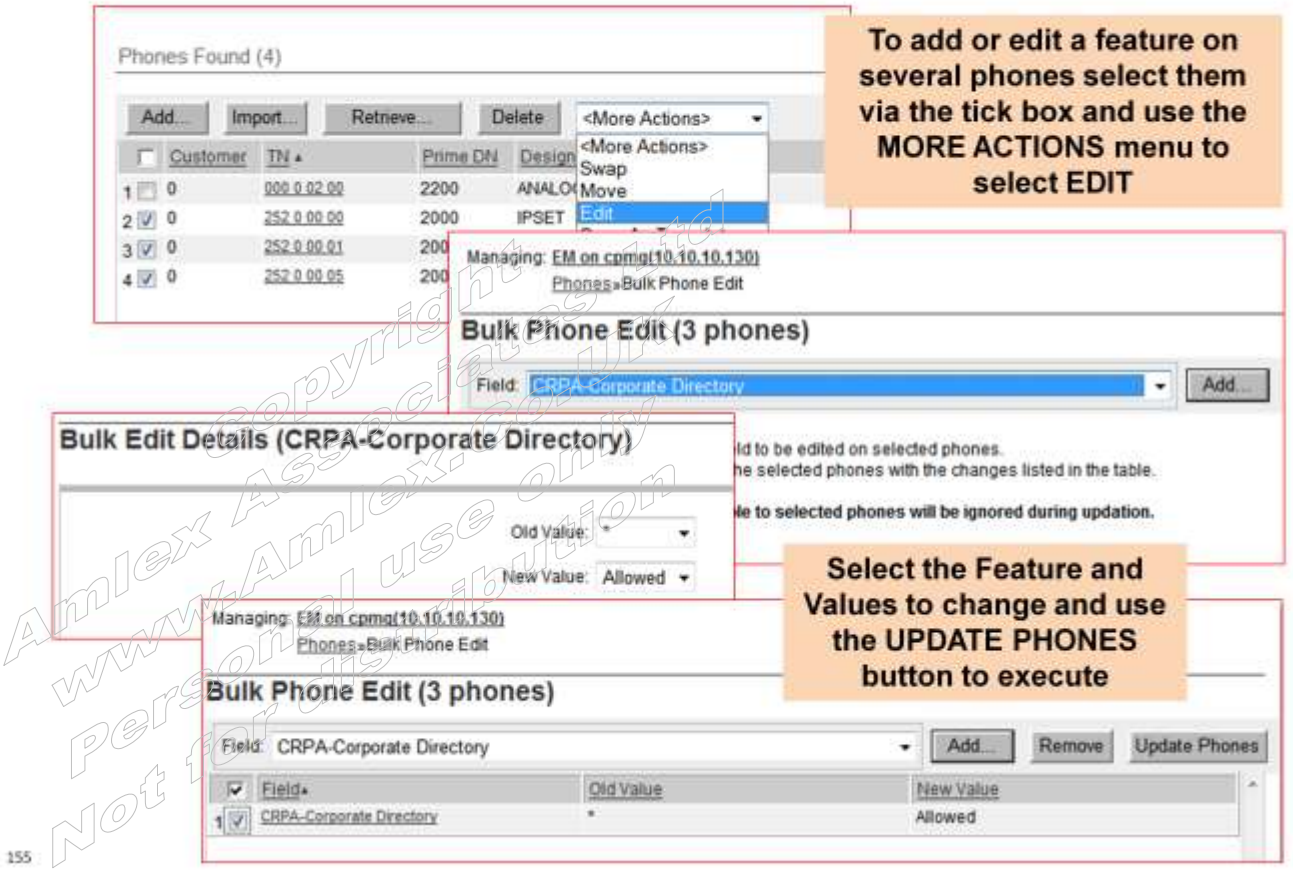
Bulk Edit of Phones

If you need to make a change or add a feature to a number of sets this can be done by selecting them using the tick box as shown in the PHONE listing.

From the drop down menu select the **EDIT** option which will move you to the second screen shown. Here you can select the field you wish to change (Here we are adding Corporate Directory access) using the **ADD** button.

You are prompted for the Old and New values to be used for the edit. Note that the * is used as a wild card for the Old value here.

Several fields can be added as shown in the lower screen shot. When you have all of the edits required select the **FIELD**s using the tick boxes on the left of the list and then execute them using the **UPDATE PHONES** button.



Notes

_____

_____

_____

_____

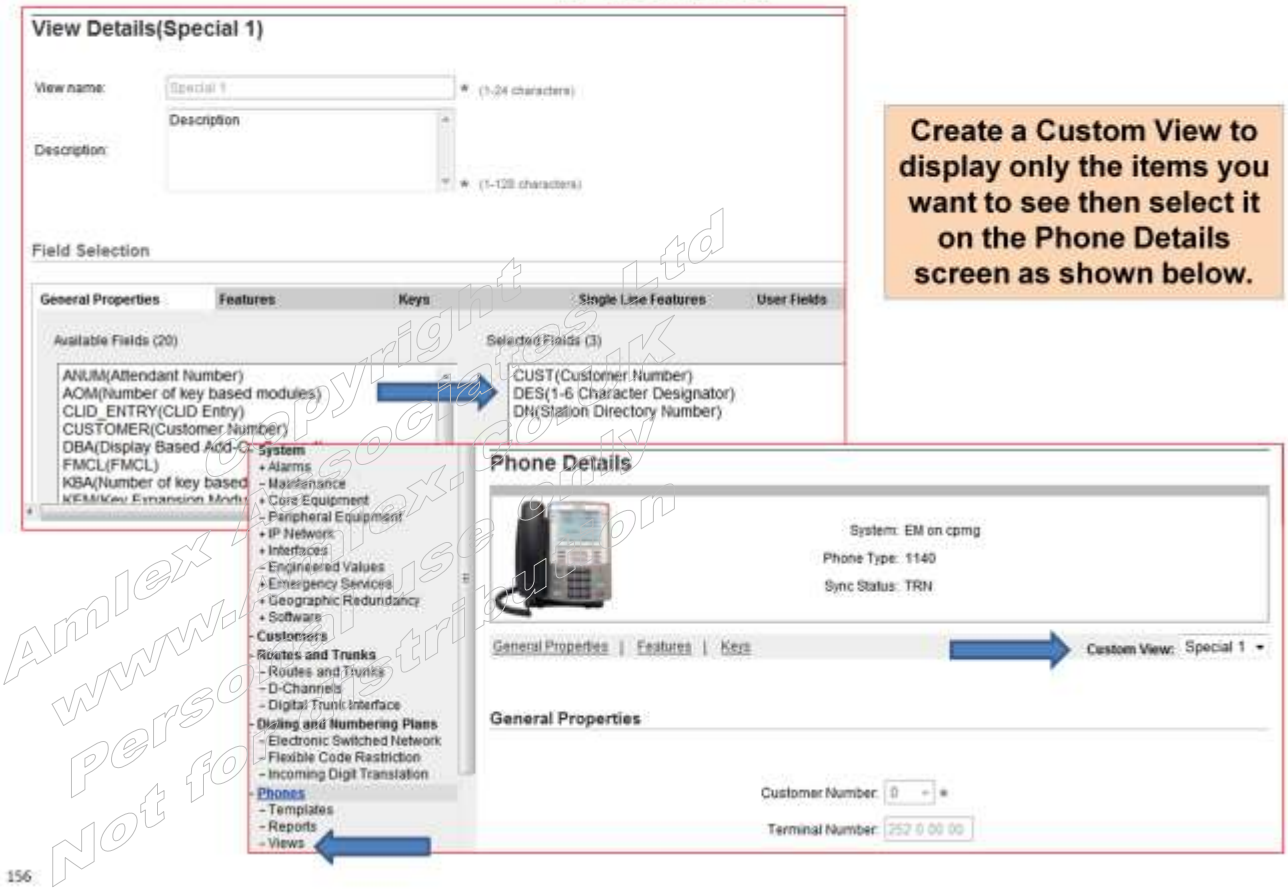
Copyright Amlex Associates Ltd

Views

Views area way of customising the pages so that only the information you wish to see is displayed on the Phone Details screen.

Create the screen you require by selecting the **VIEWS** option under the **PHONES** menu. Add a name and description and then the fields you want shown.

Now when you access the Phone Details page select the **CUSTOM VIEW** from the drop down menu on the right of the page.



Create a Custom View to display only the items you want to see then select it on the Phone Details screen as shown below.

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

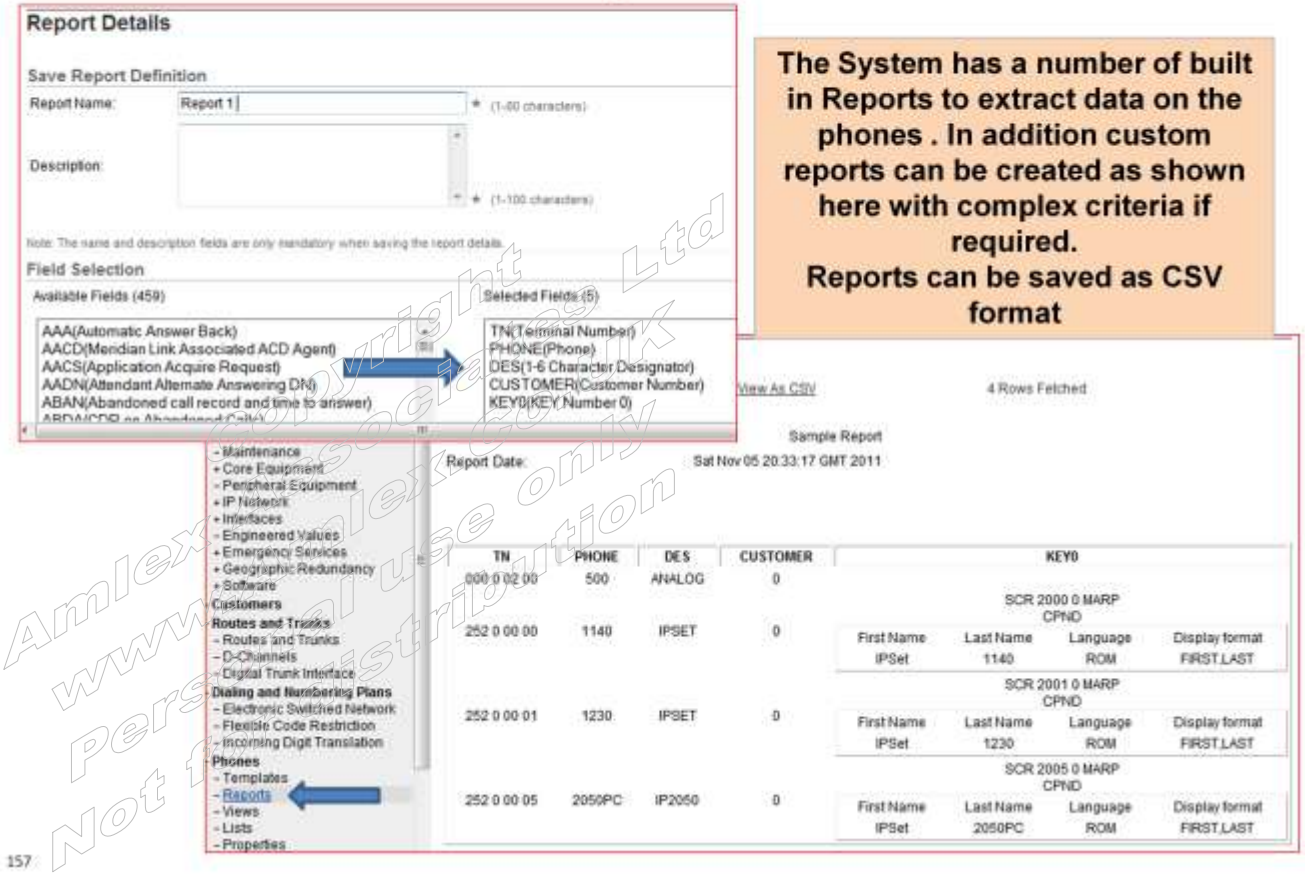
_____

Reports

Reports are a method of extracting Phone information from the system and can be displayed as HTML as shown here or as CSV information for export and subsequent manipulation.

Access the Reports screen from the **PHONES / REPORTS** menu option. Add a name and description for the report and then select the fields you want and add any criteria for selection.

When you run the report you will see it can be output for the screen or exported as a CSV file.



Amlex Associates Ltd
Copyright
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Exercise

- Use the Element Manager Phones menu to do the following
  - Create a single 1140 set with multiple DN buttons
  - Create a single 1230 set with a single DN
  - Edit an existing set and change the Name information
  - Create a Custom View to view the sets
  - Edit the file provided containing Set information and import it to your system
  - Do a Bulk Edit to add support for the Corporate Directory to you phones
  - Add a Station Control Password to IP sets
    - Ensure SCPW length is set in the Customer data
  - Create a Report to select a subset of your phones
    - Export the data created as a CSV file
    - Edit the file to change the TN's and DN's and re-import it

Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

158

Notes

_____

_____

_____

_____

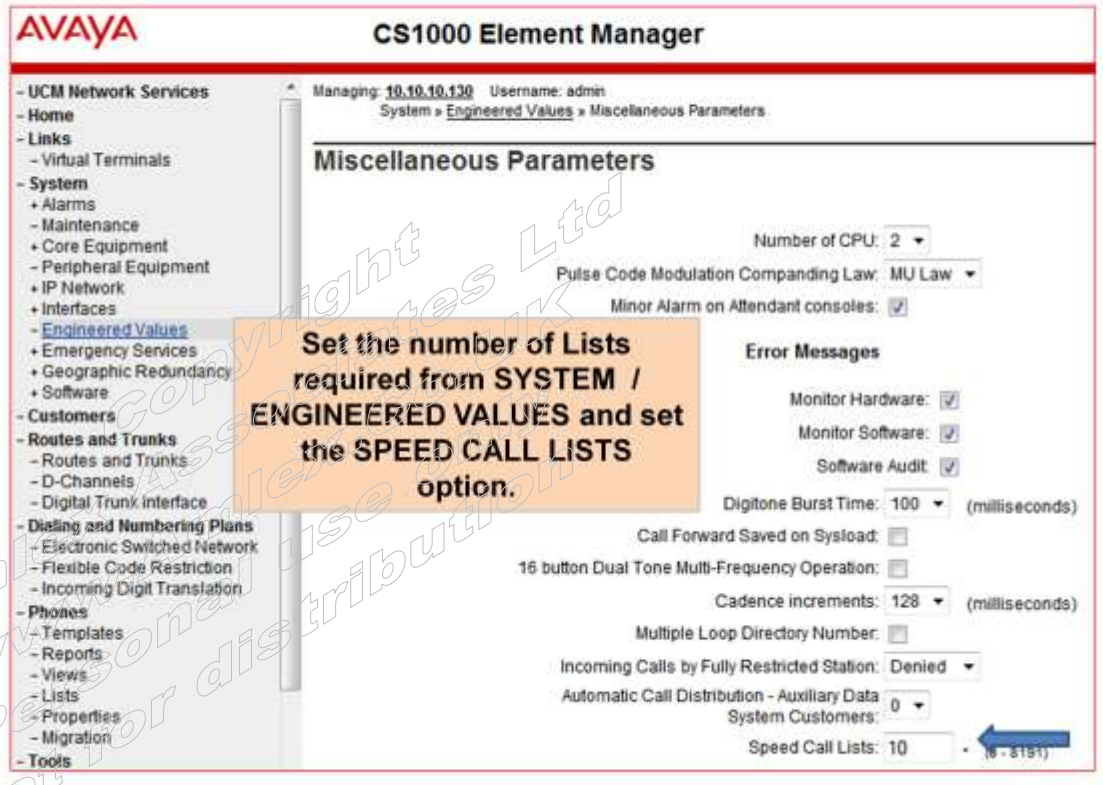
13. List Manager

If the database hasn't been configured for lists you may need to do this in overlay 17 or the Element Manager.

LD 17
CHG PARM
..
MSCL XX no of lists allowed

In Element Manager access the **ENGINEERED VALUES** menu page and then add the number of lists required in the **SPEED CALLS LIST** option.

Once this is set you will be able to add lists to the system.



159

Notes

_____

_____

_____

_____

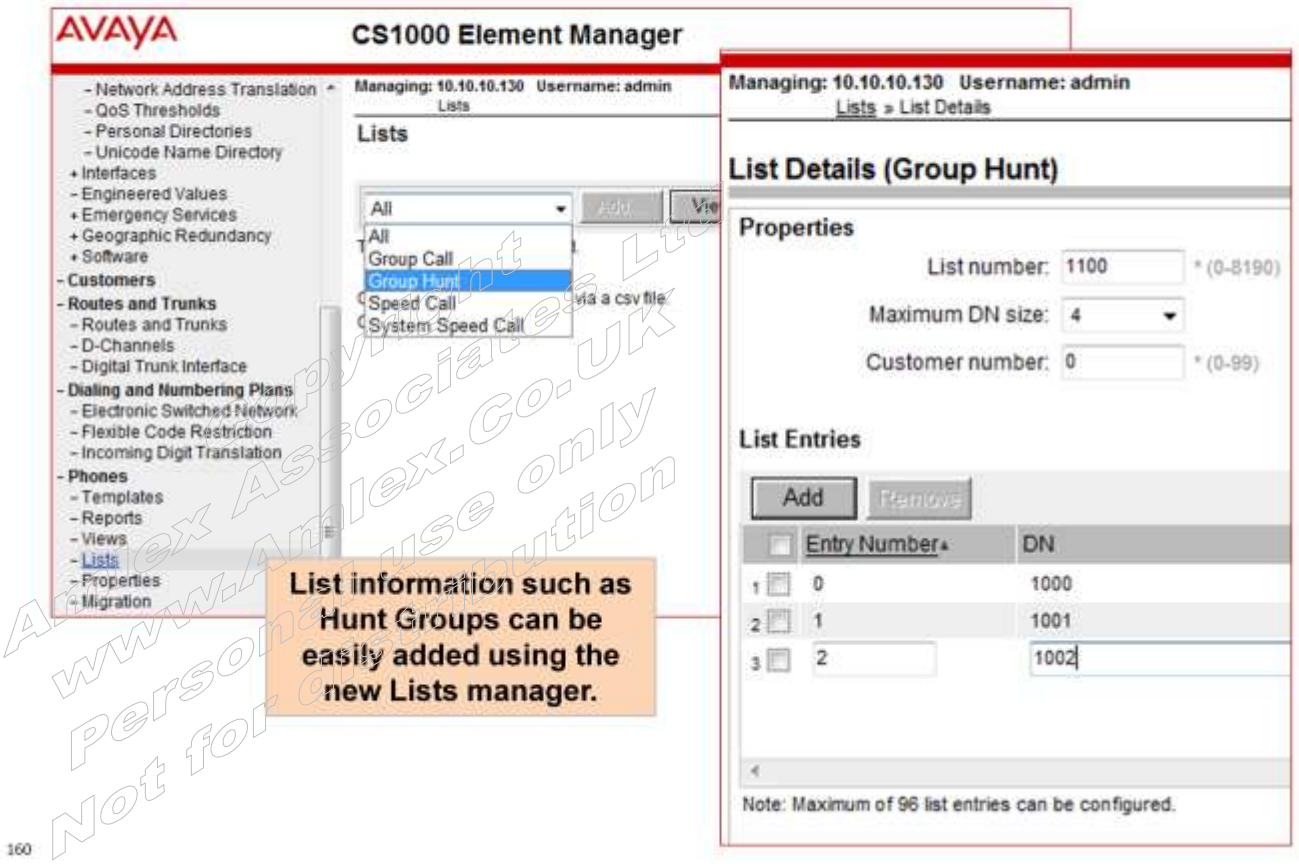
Copyright Amlex Associates Ltd

List Manager

The LISTS menu option gives the user the ability to create and manage Group Call, Group Hunt, Speed Call and System Speed Call lists.

As you can see in the example the Group Hunt list can be defined on one screen.

Firstly the List Number is entered followed by the Maximum DN size and Customer number. Then the List Entries are added to the list to complete the group.



Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

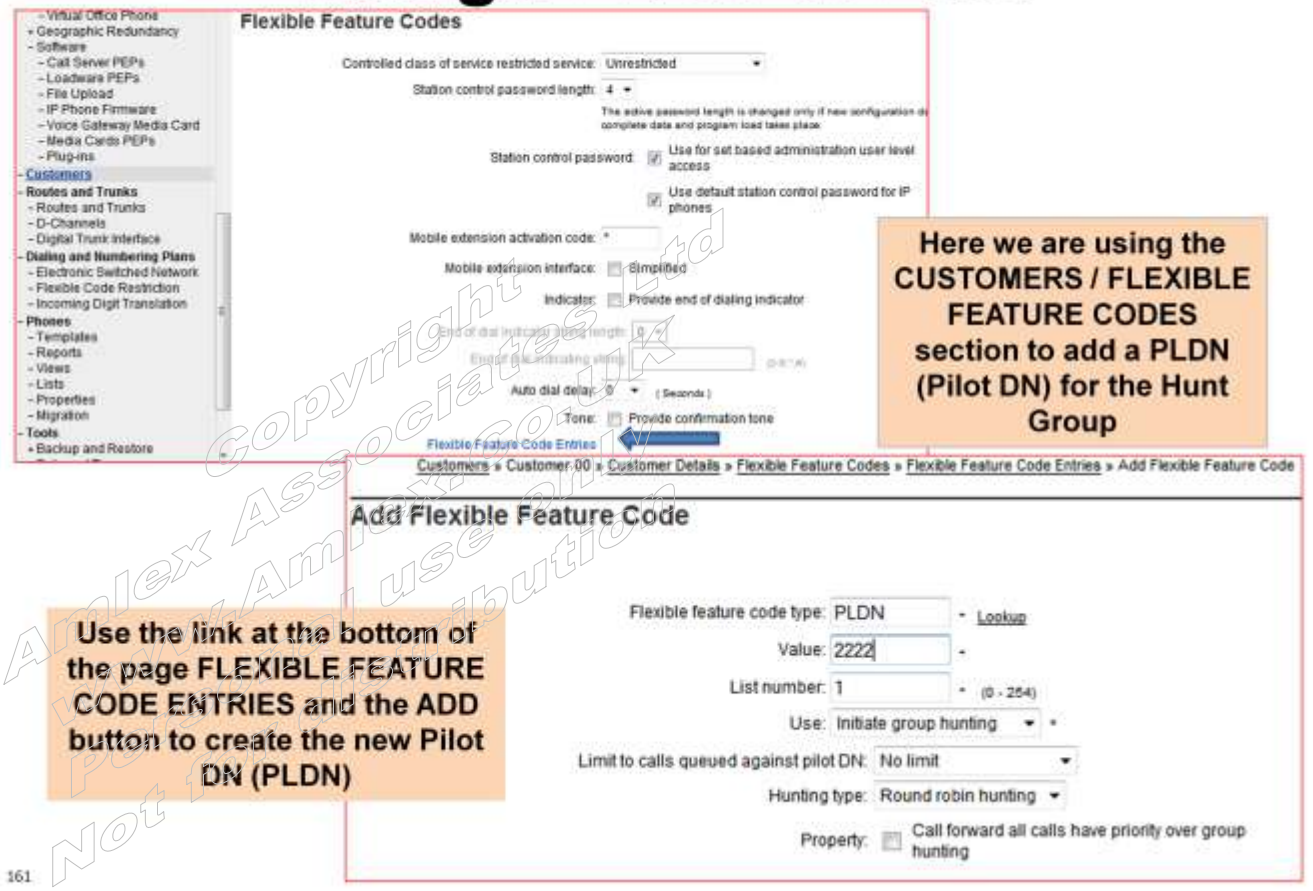
_____

Copyright Amlex Associates Ltd

Assign PLDN to List

If you are creating a Hunt Group list you will subsequently need to assign a Pilot DN (PLDN) to it. This can be done via the **CUSTOMER** menu option selecting the **FLEXIBLE FEATURE CODES** option from the main list.

Click on the link **FLEXIBLE FEATURE CODE ENTRIES** (arrowed) and then add the code type PLDN. The screen will change to show all the options required which you may then complete.


Flexible Feature Codes
Here we are using the CUSTOMERS / FLEXIBLE FEATURE CODES section to add a PLDN (Pilot DN) for the Hunt Group
Customers » Customer 00 » Customer Details » Flexible Feature Codes » Flexible Feature Code Entries » Add Flexible Feature Code
Add Flexible Feature Code
Use the link at the bottom of the page FLEXIBLE FEATURE CODE ENTRIES and the ADD button to create the new Pilot DN (PLDN)
Flexible feature code type: PLDN
Value: 2222
List number: 1
Use: Initiate group hunting
Limit to calls queued against pilot DN: No limit
Hunting type: Round robin hunting
Property: Call forward all calls have priority over group hunting

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Hunt groups use a list in the overlays which needs to be allocated, so if its a new switch you may need to define the number of lists in LD 17 before you start.

If you have lists allocated already then the next step is to define the Hunt Group in LD 18 as shown.

You will need to know the list number you are going to use, the length of the DN's included and the number of entries to be included. Then you simply add the DN entries.

Once the list is created you need to assign it to a DN (PLDN) in the system which of course must be unique. This is done in LD 57 (FFC

Hunt Groups - Overlays

- LD 17
- CHG PARM .....
- MSCL XX (no of lists allowed)

- LD 18
- REQ NEW
- TYPE GHT
- CUST 0
- LSNO (Next List Number)
- DNSZ (DN Size)
- SIZE (Size of list, entries)
- STOR 00 XXXX (XXXX = DN)
- WRT (C/R)
- STOR 01 XXXX (XXXX = DN)
- Continue with store entries until list completed.

- LD 57
- REQ CHG
- TYPE FFC
- CUST 0
- CODE PLDN
- PLDN (Pilot DN, which must be a unique)
- USE GPHT (Group Hunting)
- LSNO (List number created in LD 18)
- HTYP (RRB=Round Robin, LIN = Linear)
- CFWI (NO = Skip Extn if CFW Activated YES = Terminate on Extn if CFW Activated)
- MQUE (ALL = No limit on queued Calls 0 = No calls to be queued 1 = Maximum of 1 call queued)

Amlex Copyright
www.Amlex.co.uk
Personal use only
Not for distribution

162

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

14. Subscriber Manager

Subscriber Manager (Sub Mgr) is a mechanism to connect the Call server to external Directory systems such as Active Directory (AD) and use its information to automatically create Phone Sets allocated to a specific user.

In a full implimentation Subscribers would be created on the Primary UCM during a syncronisation with the AD. This creates entries into the Common Network Directory (CND) attached to the Sub Mgr. Changes are then processed by the Flow Through Provisioning (FTPROV) process to create Accounts (Phone sets) for the subscribers on Call Servers (Elements) manageg by the UCM.

Control is complete and the deletion of a Subscriber will delete the attached Account(Phone set) on the call server.

Some definitions used by Sub Mgr.

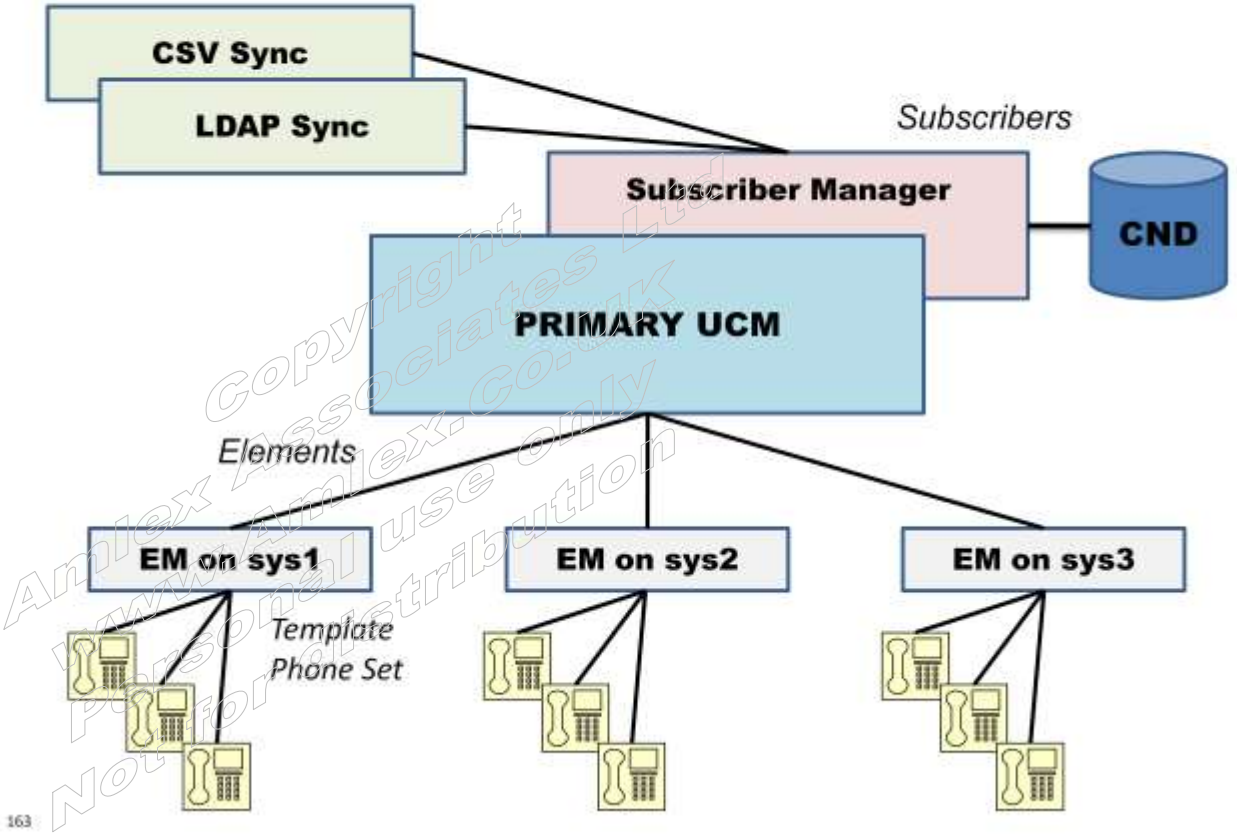
Subscriber
- User or Project

Account
- Telephony Account ot Phone Set

Element
- Call Server

Target
- Customer on Call Server

Template
- Phone Template for common functions



Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Create a Template in BCC

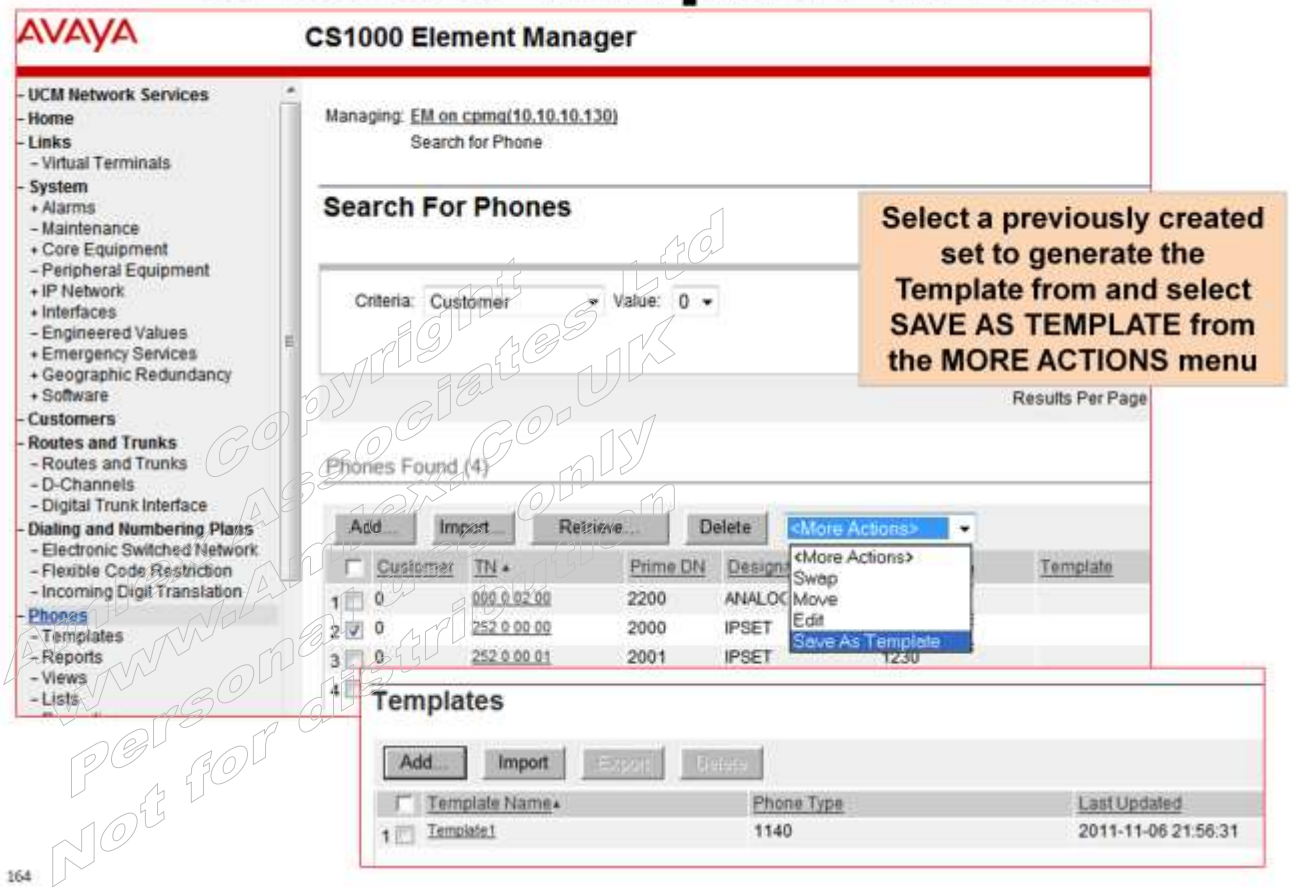
To use Sub Mgr, we must have a Set Template configured in the Element manager BCC.

This is used to generate the sets without user intervention, selecting TN and DN automatically.

To create a Template we can use an existing set that has the features we require and then use the **MORE ACTIONS** drop down menu in the **PHONES** listing screen shown here. Select the set you want with the tick box as shown and then select the **SAVE AS TEMPLATE** option from the drop down menu.

You can then add a name to the template and add any changes required before saving it. Be sure to check the Template works correctly before using it with Sub Mgr.

For use with Subscriber Manager you will need to add the starting number of the DN range to use as the Prime DN on key 0 i.e. If you want numbers in the 2XXX range add Key 0 as an SCR DN 2000



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

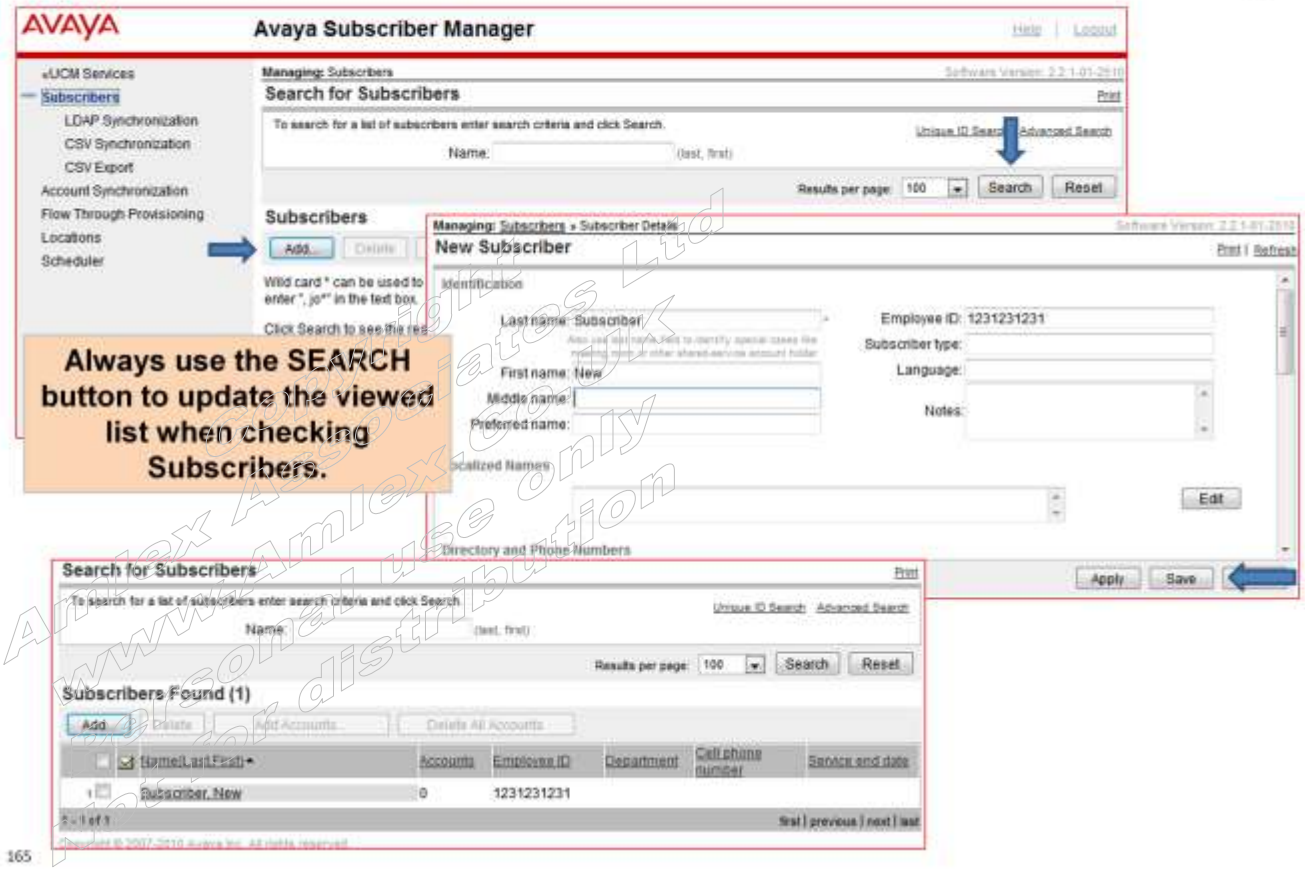
Adding New Subscribers Manually

Subscribers can be added manually to the system is you are not linked to an external directory.

Select the **SUBSCRIBERS** menu option and then the **ADD** button to create a new user. Add the information required, Last Name, First name etc and then **SAVE** it.

Each Subscriber is assigned a Unique User ID (UUID) to ensure it is correctly filed and retrieved by the system.

In the lower screen you can see the completed Subscriber with the name underlined as it is a link which maybe clicked on to edit the content. In addition you will see that the Accounts field is currently showing 0 as there is no set assigned to the Subscriber.



165

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add an Account to Subscriber

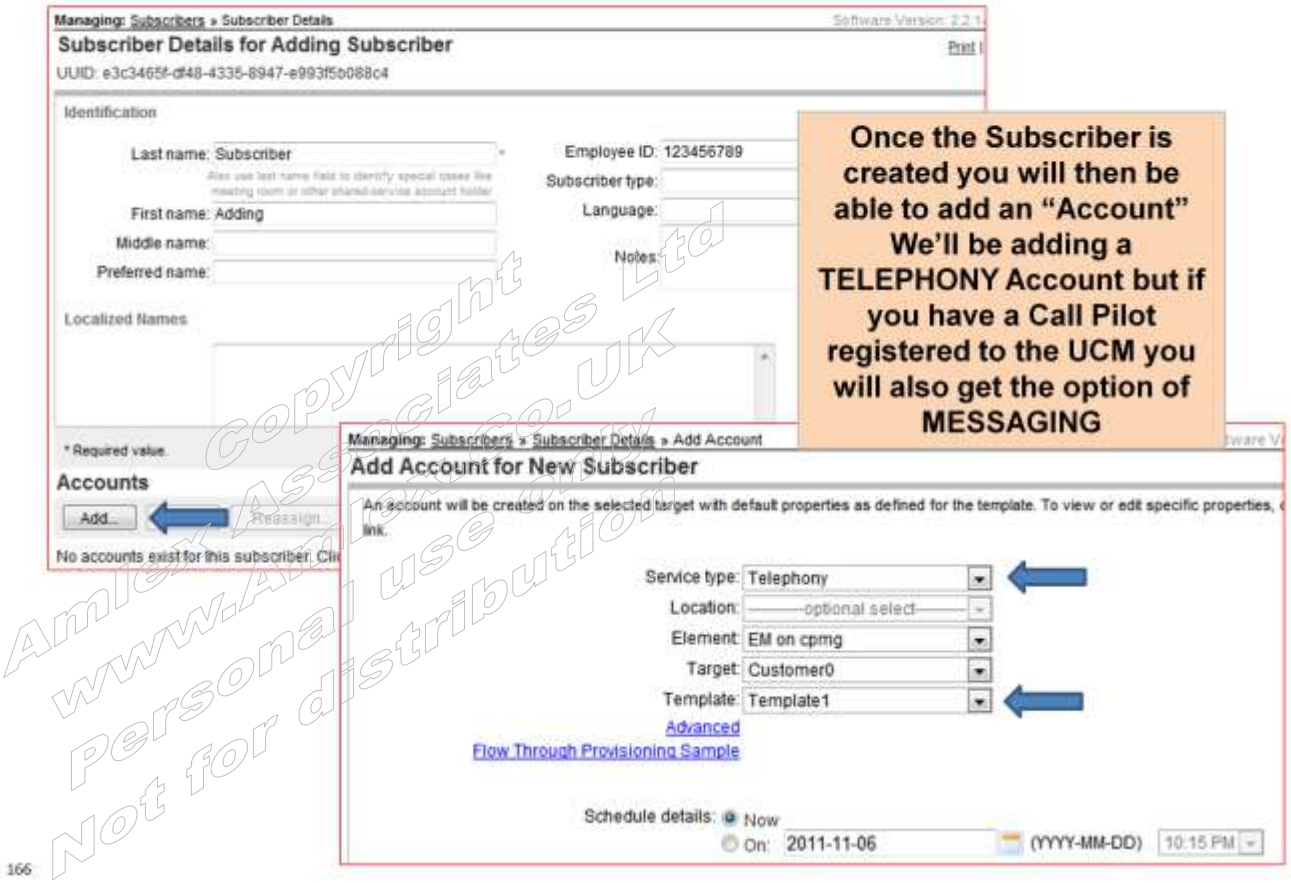
To add an Account to the subscriber click on the link to go to the details page and then click on the **ADD** button under the **ACCOUNTS** section bottom left of the display.

Note also the **REASSIGN** and **DISASSOCIATE** buttons which allow you to move or sever the link between and account and a Subscriber. Remember if the subscriber is deleted any associated account (Phone Set) will also be deleted. Thus to preserve a Phone Set whilst removing a subscriber you must either reassign or disassociate the account before the deletion.

From the Add Account screen select **TELEPHONY** from the **SERVICE TYPE** drop down menu. On UCM systems where a Call Pilot has been added to the Element list there a Messaging option will also be available.

Select the correct **ELEMENT** , **TARGET**, and **TEMPLATE** and then click **SAVE** and the system will create a new Phone Set allocated to the subscriber.

Note the **ADVANCED** link which allows you to jump to the BCC screens to edit the set before completion. Also you can choose to create the set at a later time by selecting the **DATE** and **TIME** from the drop down menus and selecting the radio button **ON**.


Managing: Subscribers » Subscriber Details
Subscriber Details for Adding Subscriber
UUID: e3c3465f-df48-4335-8947-e993f5b088c4
Identification
Last name: Subscriber
First name: Adding
Middle name:
Preferred name:
Employee ID: 123456789
Subscriber type:
Language:
Notes:
Localized Names
* Required value.
Accounts
Add...
Reassign
No accounts exist for this subscriber.
Once the Subscriber is created you will then be able to add an "Account" We'll be adding a TELEPHONY Account but if you have a Call Pilot registered to the UCM you will also get the option of MESSAGING
Managing: Subscribers » Subscriber Details » Add Account
Add Account for New Subscriber
An account will be created on the selected target with default properties as defined for the template. To view or edit specific properties,
link.
Service type: Telephony
Location: ----------optional select----------
Element: EM on cpmg
Target: Customer0
Template: Template1
Advanced
Flow Through Provisioning Sample
Schedule details: Now
On: 2011-11-06 (YYYY-MM-DD) 10:15 PM

166

Notes

_____

_____

_____

_____

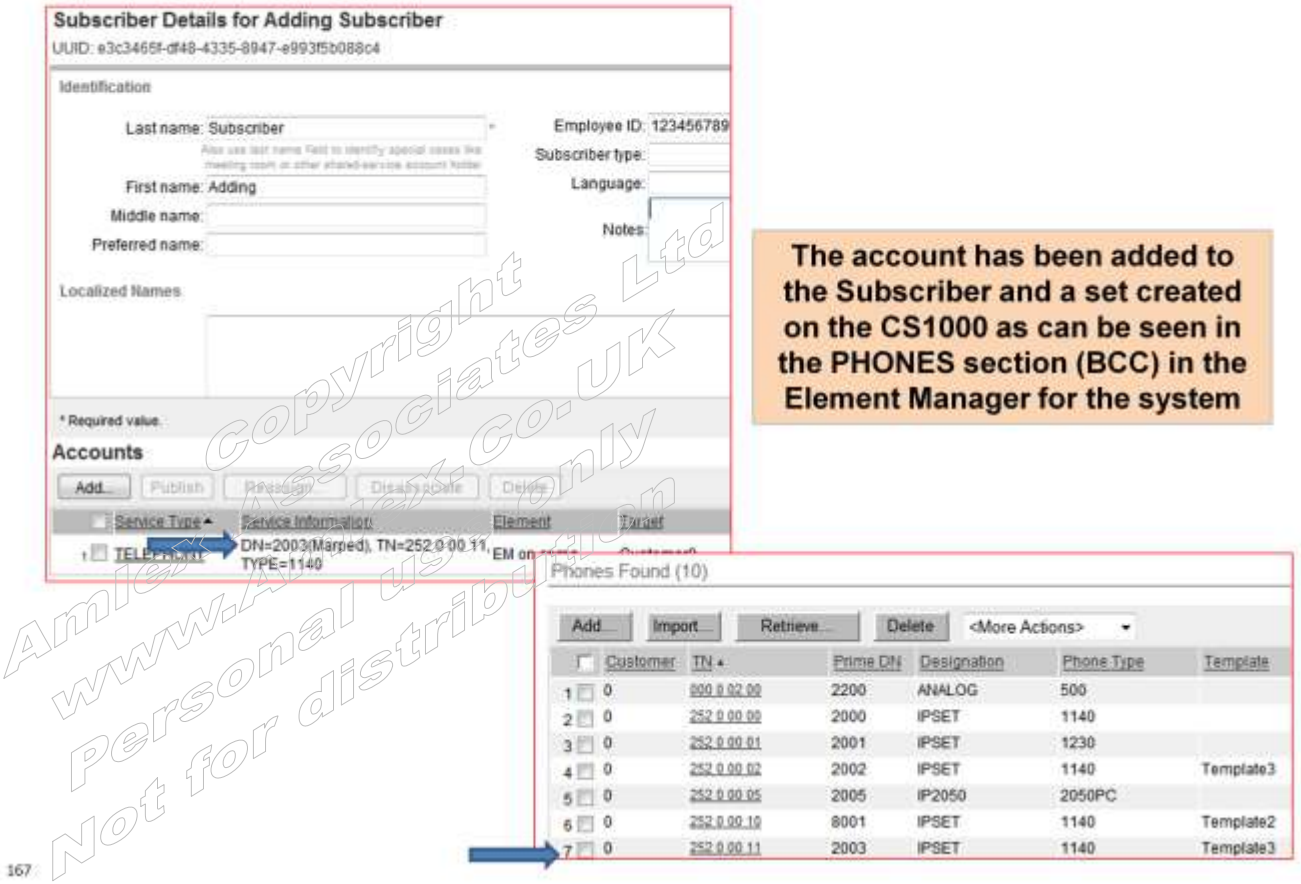
Copyright Amlex Associates Ltd

Subscriber with Account

Here you can see the created account in both the Subscriber manager screen and also the Element Manager BCC Phones list.

Note that the Phones list shows the Template that was used to create the set.

If you scroll through the subscriber information you will see that the assigned DN has been added to the record.


Subscriber Details for Adding Subscriber
UUID: e3c3465f-df48-4335-8947-e993f5b088c4
Identification
Last name: Subscriber
First name: Adding
Middle name:
Preferred name:
Employee ID: 123456789
Subscriber type:
Language:
Notes:
Localized Names
* Required value.
Accounts
Add... Publish Reassign Disassociate Delete
Service Type
Service Information
Element
Target
DN=2003(Marped), TN=252 0 00 11, TYPE=1140
EM on
The account has been added to the Subscriber and a set created on the CS1000 as can be seen in the PHONES section (BCC) in the Element Manager for the system
Phones Found (10)
Add... Import... Retrieve... Delete <More Actions>
Customer TN Prime DN Designation Phone Type Template
1 0 000 0 02 00 2200 ANALOG 500
2 0 252 0 00 00 2000 IPSET 1140
3 0 252 0 00 01 2001 IPSET 1230
4 0 252 0 00 02 2002 IPSET 1140 Template3
5 0 252 0 00 05 2005 IP2050 2050PC
6 0 252 0 00 10 8001 IPSET 1140 Template2
7 0 252 0 00 11 2003 IPSET 1140 Template3
167

Copyright Amlex Associates Ltd
Personal use only
Not for distribution

Notes

_____

_____

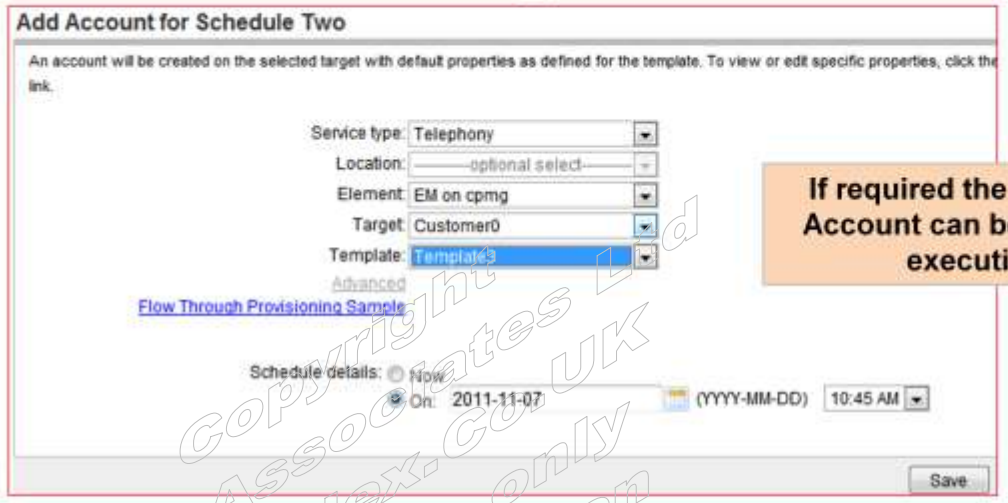
_____

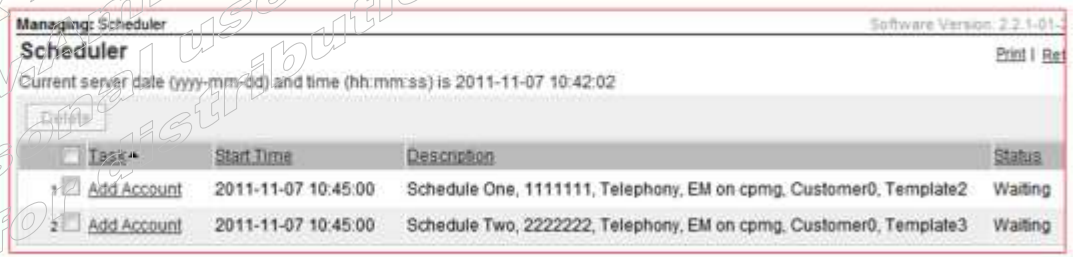
_____

Sub Mgr Scheduler

Using the scheduler as shown in the upper screen shot allow you to add phones at a later point. This is more in line with Telephony Manager's batch type approach.

Here you can see two sets waiting to be completed in the scheduler list. If necessary they can be deleted from the list if they are not required.


Add Account for Schedule Two
An account will be created on the selected target with default properties as defined for the template. To view or edit specific properties, click the link.
Service type: Telephony
Location: ----optional select----
Element: EM on cpmg
Target: Customer0
Template: Template3
Advanced
Flow Through Provisioning Sample
Schedule details: Now
On: 2011-11-07 (YYYY-MM-DD) 10:45 AM
Save
If required the creation of the Account can be scheduled for execution later.


Managing: Scheduler
Scheduler
Current server date (yyyy-mm-dd) and time (hh:mm:ss) is 2011-11-07 10:42:02
Delete
Task
Start Time
Description
Status
1 Add Account 2011-11-07 10:45:00 Schedule One, 1111111, Telephony, EM on cpmg, Customer0, Template2 Waiting
2 Add Account 2011-11-07 10:45:00 Schedule Two, 2222222, Telephony, EM on cpmg, Customer0, Template3 Waiting

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

168

Notes

_____

_____

_____

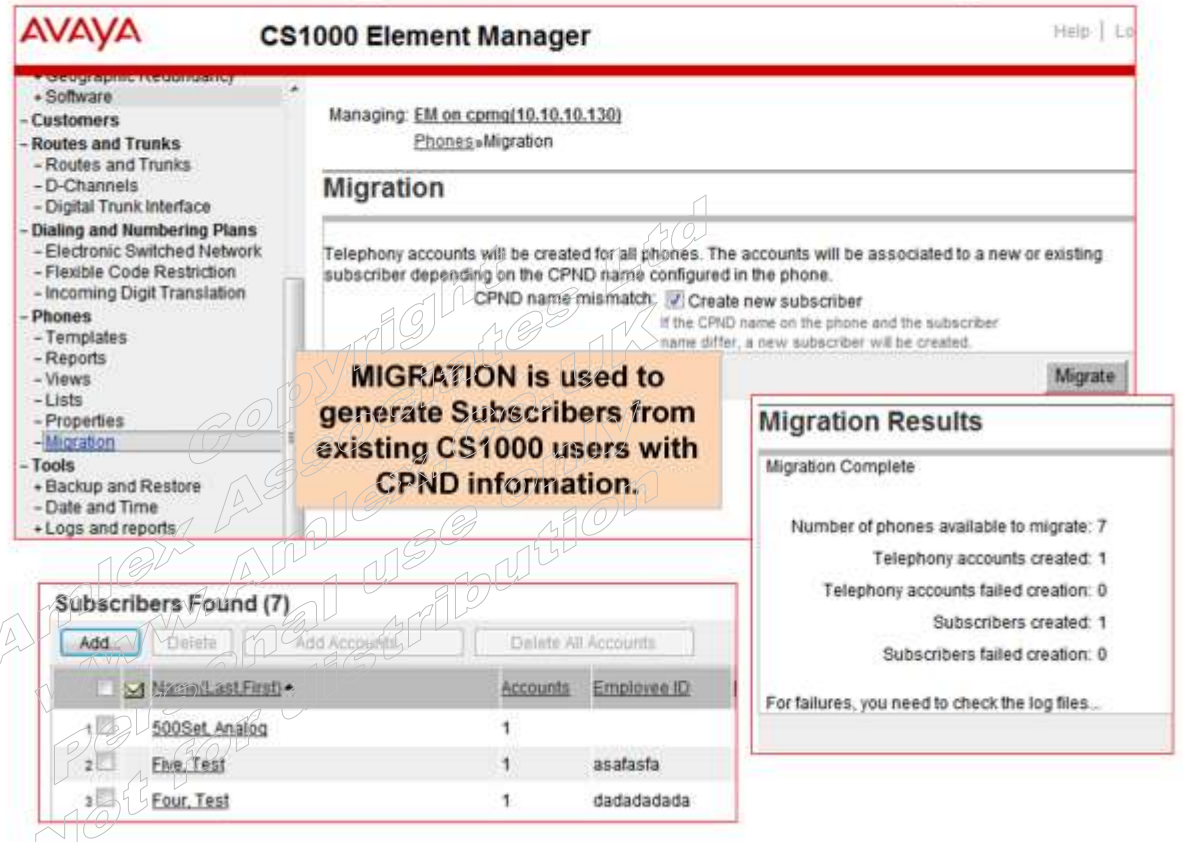
_____

Migration to Sub Mgr

Another way to create subscribers is from the Phones and associated Call Party Name Display (CPND) information already configured on the call server. This is usually a one off event but can be repeated is required.

To run the Migration task select **PHONES / MIGRATION** from the Element Manager of the system you are working on. Tick the box to create new subscribers from CPND information and then click the **MIGRATE** button.

A display similar to that on the right will be seen and sets with unique CPND information will be created as new subscribers in the Subscriber Manager as shown on the lower screen shot.


AVAYA
CS1000 Element Manager
Help | Lo
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
- Tools
+ Backup and Restore
- Date and Time
+ Logs and reports
Managing: EM on cpmg(10.10.10.130)
Phones »Migration
Migration
Telephony accounts will be created for all phones. The accounts will be associated to a new or existing subscriber depending on the CPND name configured in the phone.
CPND name mismatch: Create new subscriber
If the CPND name on the phone and the subscriber name differ, a new subscriber will be created.
Migrate
MIGRATION is used to generate Subscribers from existing CS1000 users with CPND information.
Migration Results
Migration Complete
Number of phones available to migrate: 7
Telephony accounts created: 1
Telephony accounts failed creation: 0
Subscribers created: 1
Subscribers failed creation: 0
For failures, you need to check the log files...
Subscribers Found (7)
Add...
Delete
Add Accounts...
Delete All Accounts
Name(Last,First)
Accounts
Employee ID
500Set, Analog 1
Five, Test 1 asafasfa
Four, Test 1 dadadadada

Amlex Associates Ltd Copyright Protected Personal use only Not for distribution

169

Notes

_____

_____

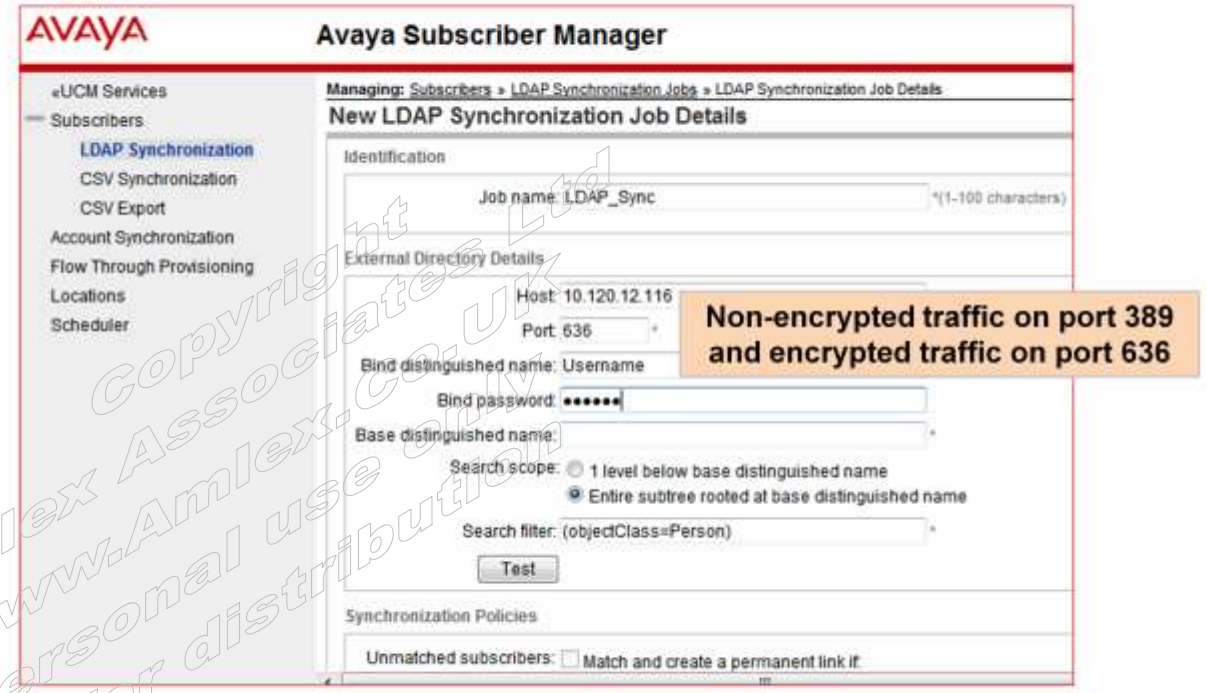
_____

_____

LDAP Synchronisation

Ultimately for a completely automated solution the subscriber manager would be linked to an LDAP server using a synchronisation job as shown here. We configure the LDAP server detail and how we wish to connect with login details etc and also the Search Scope we may need to use to align the UCM and LDAP entries.

There is a **TEST** button to check that the connection is made correctly but once the information is correctly established the synchronisation would occur periodically thus updating the CND. These updates are then processed by Subscriber Manager and implemented using the Flow Through Provisioning mentioned earlier.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

170

Notes

_____

_____

_____

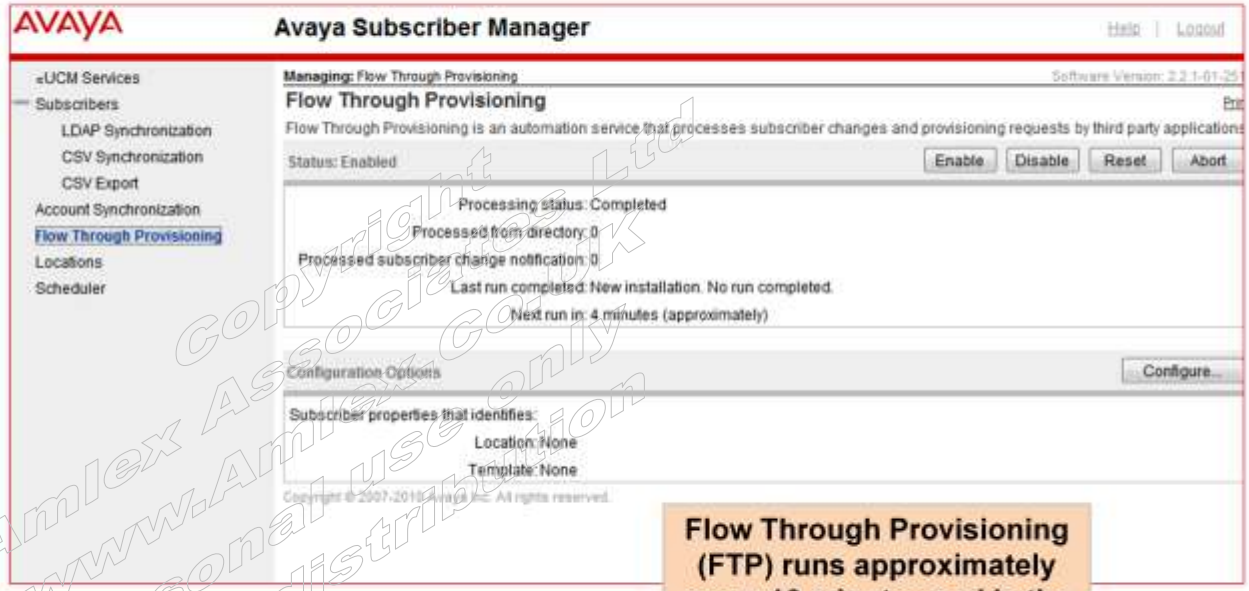
_____

Flow Through Provisioning

Flow Through Provisioning (FTPROV) is a background task which when enabled runs every 10 minutes approximately and executes any changes to the subscribers.

Thus if an LDAP update had added new users these would then be created by FTPROV on the appropriate systems automatically.

Make sure the FTPROV is running and if not use the **ENABLE** button to start it.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Flow Through Provisioning (FTP) runs approximately every 10 minutes and is the mechanism used to process changes and additions.

171

Notes

_____

_____

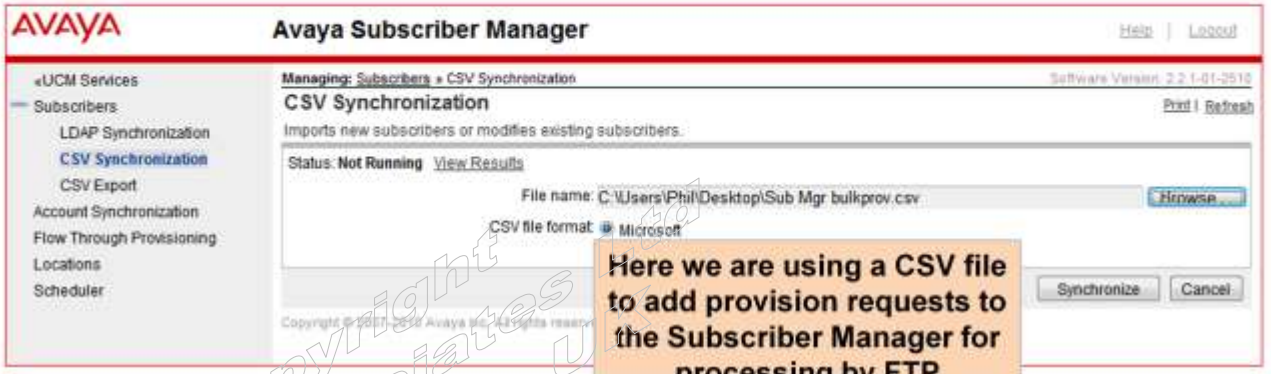
_____

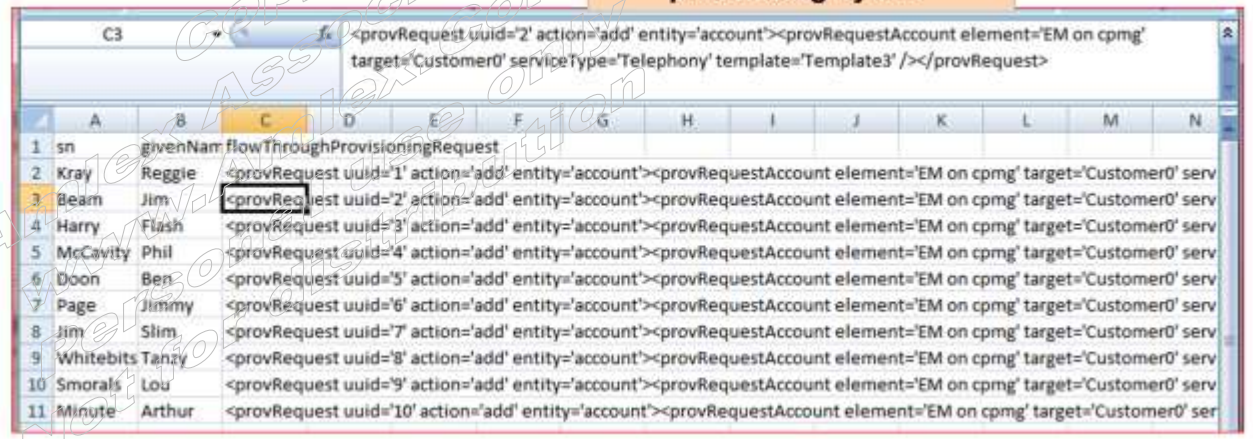
_____

CSV Synchronisation

Another option available is the use of an imported CSV format file rather than an online synchronise.

Here we have a Bulk Provision file which has the provision requests included in it. By importing this to subscriber manager using the **SYNCHRONISE** button, subscribers will be created as can be seen on the next page. However at this stage they have no associated account although the information is there to create it.





C3 <provRequest uuid='2' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serviceType='Telephony' template='Template3' /></provRequest>

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	sn	givenNam	flowThroughProvisioningRequest											
2	Kray	Reggie	<provRequest uuid='1' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
3	Beam	Jim	<provRequest uuid='2' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
4	Harry	Flash	<provRequest uuid='3' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
5	McCavity	Phil	<provRequest uuid='4' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
6	Doon	Ben	<provRequest uuid='5' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
7	Page	Jimmy	<provRequest uuid='6' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
8	Jim	Slim	<provRequest uuid='7' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
9	Whitebits	Tanzy	<provRequest uuid='8' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
10	Smorals	Lou	<provRequest uuid='9' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' serv											
11	Minute	Arthur	<provRequest uuid='10' action='add' entity='account'><provRequestAccount element='EM on cpmg' target='Customer0' ser											

172

Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Internal use only
Not for distribution

Notes

_____

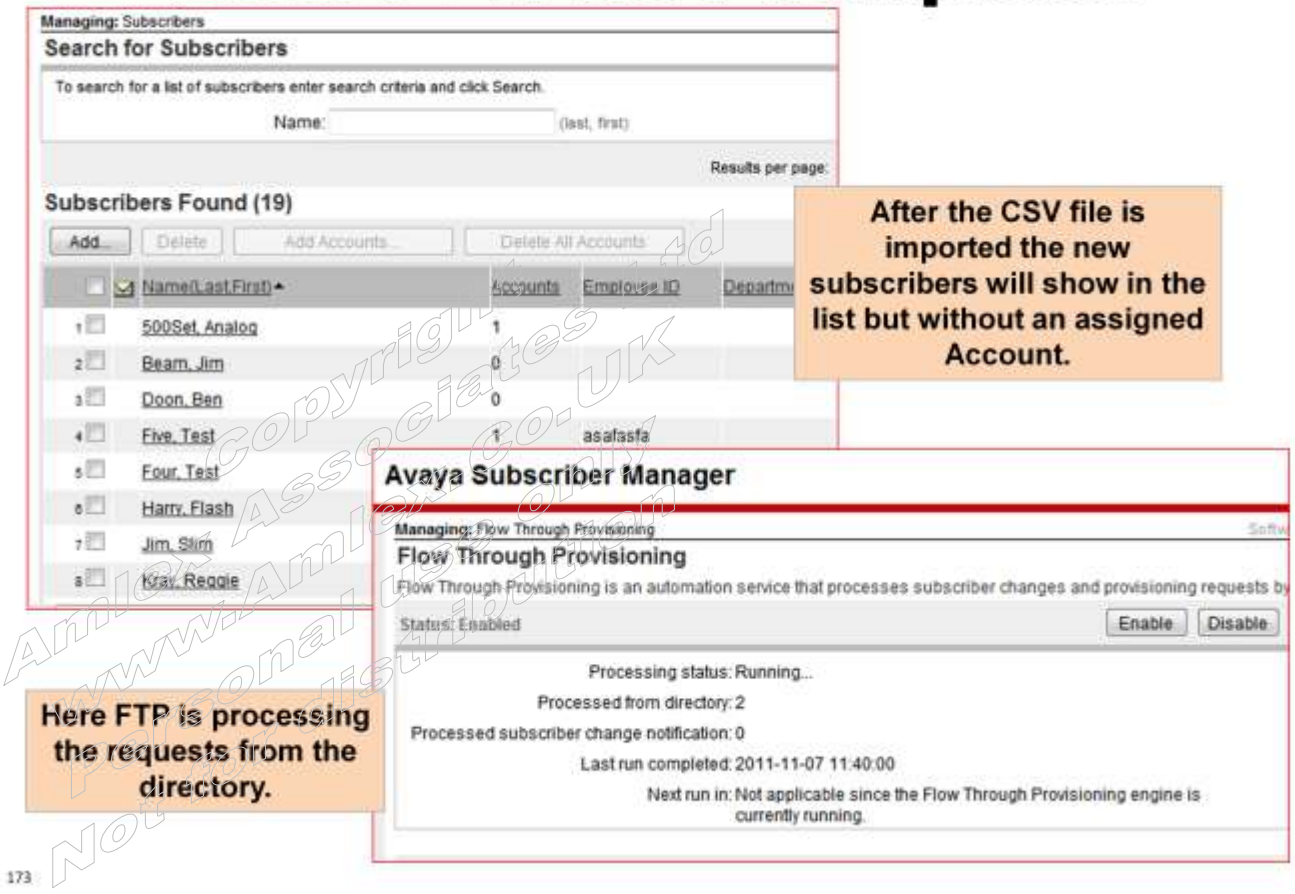
_____

_____

_____

Here you can see the list of subscribers which has a number with no allocated account. These are the imported subscribers and when the FTPROV runs as shown in the lower screen the accounts will be created on the Call server itself.

Before FTPROV Completes


Managing: Subscribers
Search for Subscribers
To search for a list of subscribers enter search criteria and click Search.
Name:
(last, first)
Results per page:
Subscribers Found (19)
Add...
Delete
Add Accounts...
Delete All Accounts
Name(Last,First)
Accounts
Employee ID
1 500Set, Analog 1
2 Beam, Jim 0
3 Doon, Ben 0
4 Five, Test 1 asafasfa
5 Four, Test
6 Harry, Flash
7 Jim, Slim
8 Kray, Reggie
After the CSV file is imported the new subscribers will show in the list but without an assigned Account.
Avaya Subscriber Manager
Managing: Flow Through Provisioning
Flow Through Provisioning
Flow Through Provisioning is an automation service that processes subscriber changes and provisioning requests by
Status: Enabled
Enable
Disable
Processing status: Running...
Processed from directory: 2
Processed subscriber change notification: 0
Last run completed: 2011-11-07 11:40:00
Next run in: Not applicable since the Flow Through Provisioning engine is currently running.
Here FTP is processing the requests from the directory.
173

Notes

_____

_____

_____

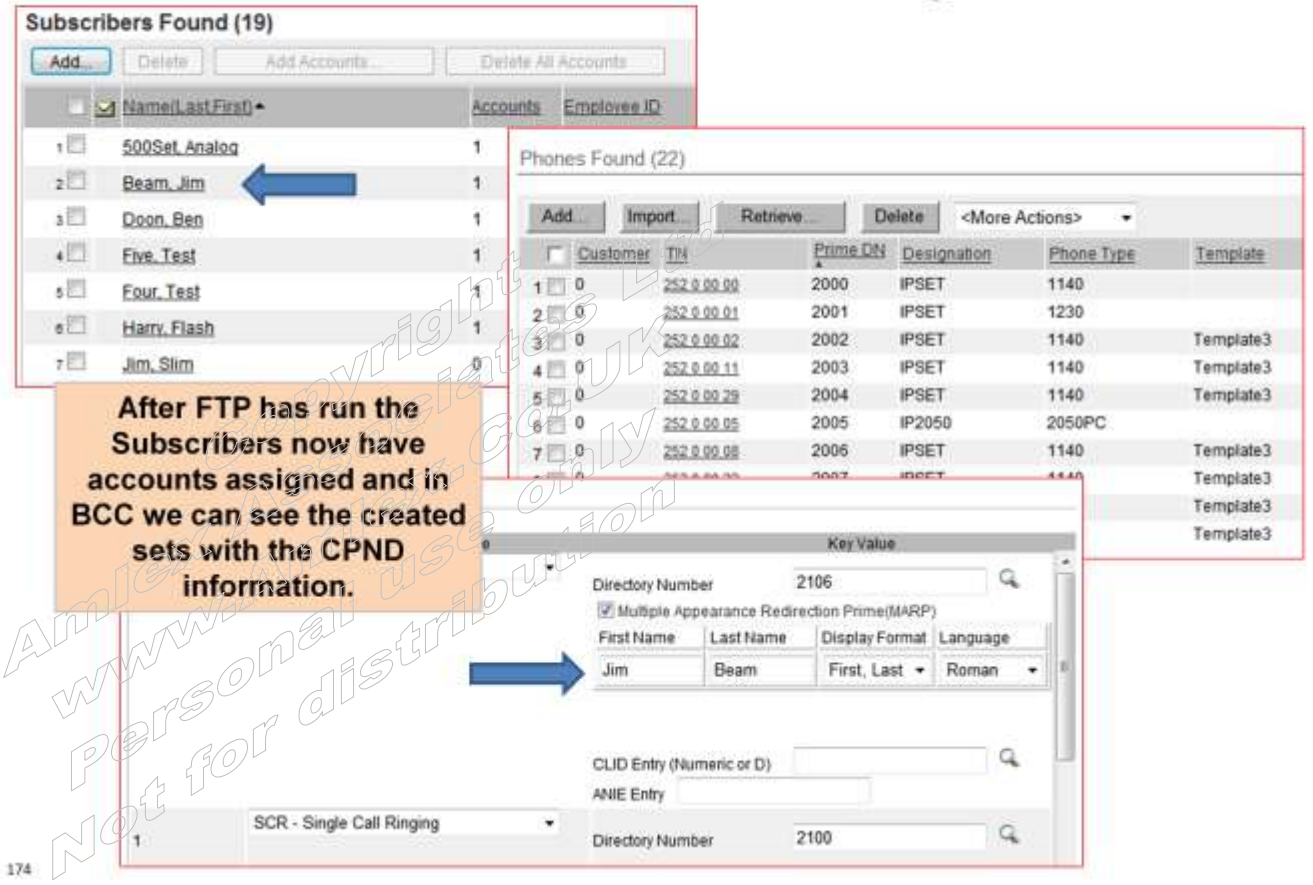
_____

Copyright Amlex Associates Ltd

Provisioned in Sub Mgr/BCC

Here we can see the fully provisioned subscribers showing an assigned account in the Subscribers list.

In the Element Manager BCC we can see the sets created and looking at the detail we can see the Subscriber name has been assigned to the Prime DN of the created set.



Notes

_____

_____

_____

_____

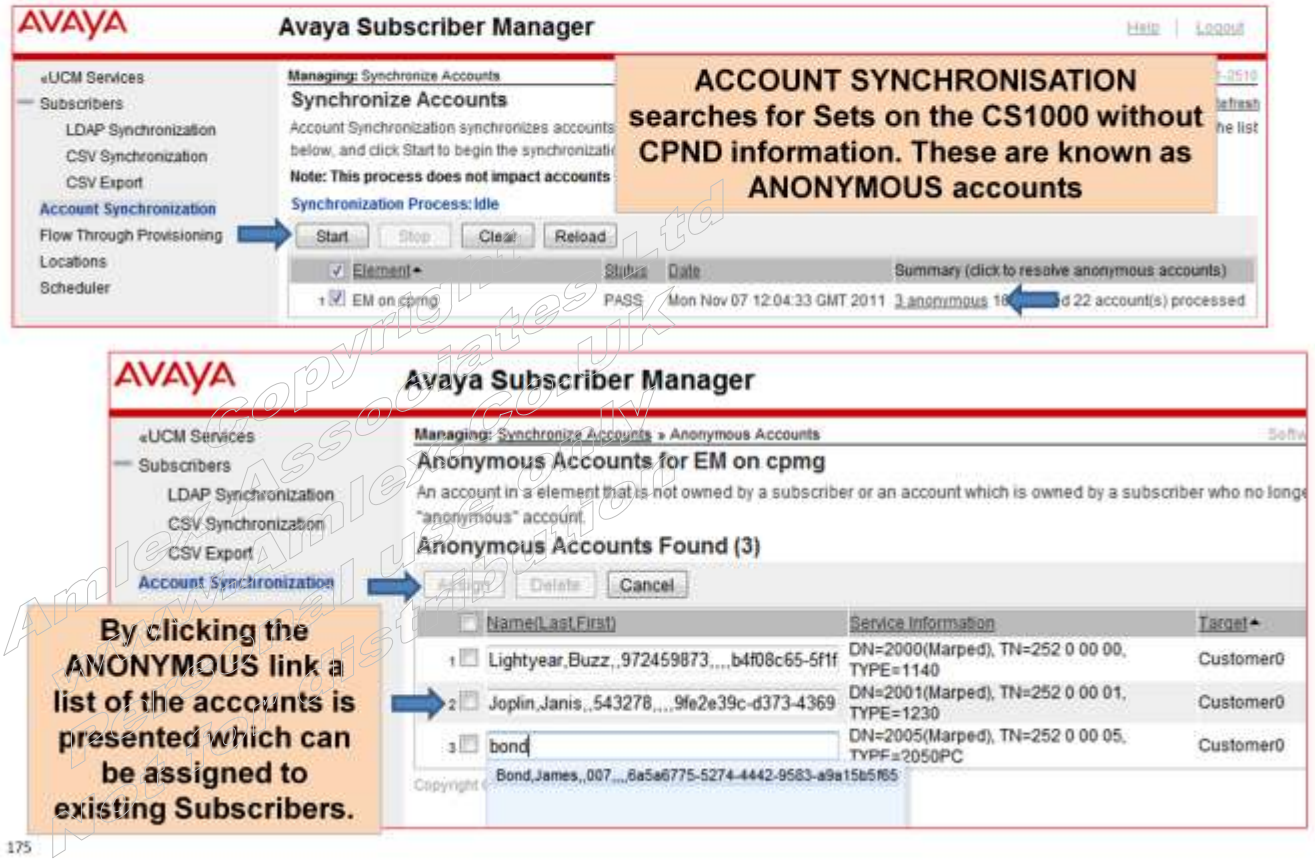
Copyright Amlex Associates Ltd

Account Synchronisation

One final option is to allocate Phone sets without CPND information to a subscriber. This is done using the Account Synchronisation option shown here.

Select the system to synchronise using the tick box as shown in the upper screen shot. Then click the **START** button to find all Phone sets without CPND information. These are known as Anonymous accounts and once the process completes you can click on the **x anonymous** link to see the list of sets to be assigned. (Lower screenshot)

Its now a case of typing in the first few letters of subscriber you wish to allocate to the account as shown and selecting them. Once the list is complete select the accounts with the tick box and click on the **ASSIGN** button to complete the link between the two entities.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Exercise

- Create six New Subscribers Manually
  - Add accounts to two of them manually
  - Use the advanced option to create an account for a third subscriber
  - Add an account using the scheduler to a fourth
  - Check the sets have been created correctly in Element manager
- From Element Manager BCC
  - Migrate sets with CPND info to Sub Mgr
- Edit the "bulkprov" file provided changing
  - EM on sysX & Template to suit your system
  - Enable FTPROV
  - Import the file and check FTPROV for Account creation
  - Check created sets in Element Manager
- Run ACCOUNT SYNCRONISATION
  - Assign Subscribers without accounts to Anonymous accounts
- Remove Subscribers from the list
  - Delete Subscriber without changing Account and check Set is removed
  - Use REASSIGN & DISASSOCIATE buttons to preserve Account when subscriber is deleted.

176

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

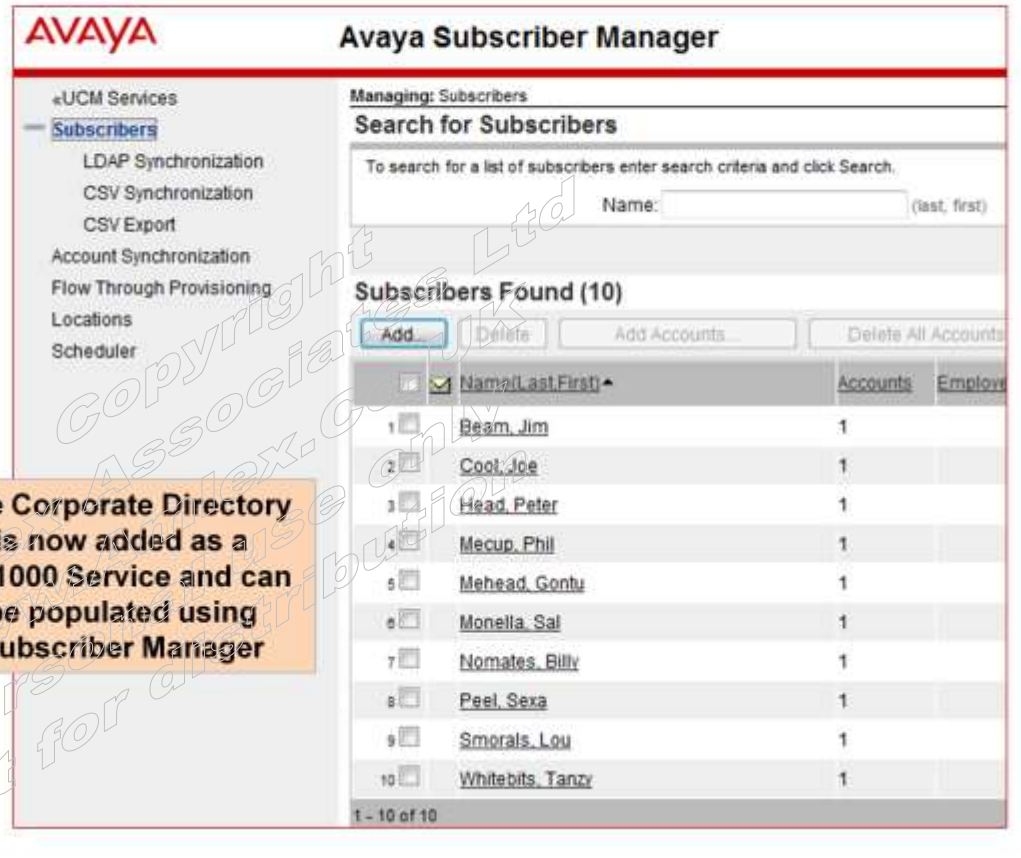
_____

15. Corporate Directory

With the demise of Telephony Manager we lose the option to enter the Corporate Directory. Thus on Rel 7 there is a new **CS1000 SERVICES** option for **CORPORATE DIRECTORY**.

In order to use the Corporate Directory we need to use the Subscriber Manager to manage entries.

Entries can be made manually, via CSV import or via synchronisation with an LDAP database. Alternatively entries can be generated from the existing CPND entries on the Call Server using the **PHONES / MIGRATION** option in Element manager.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

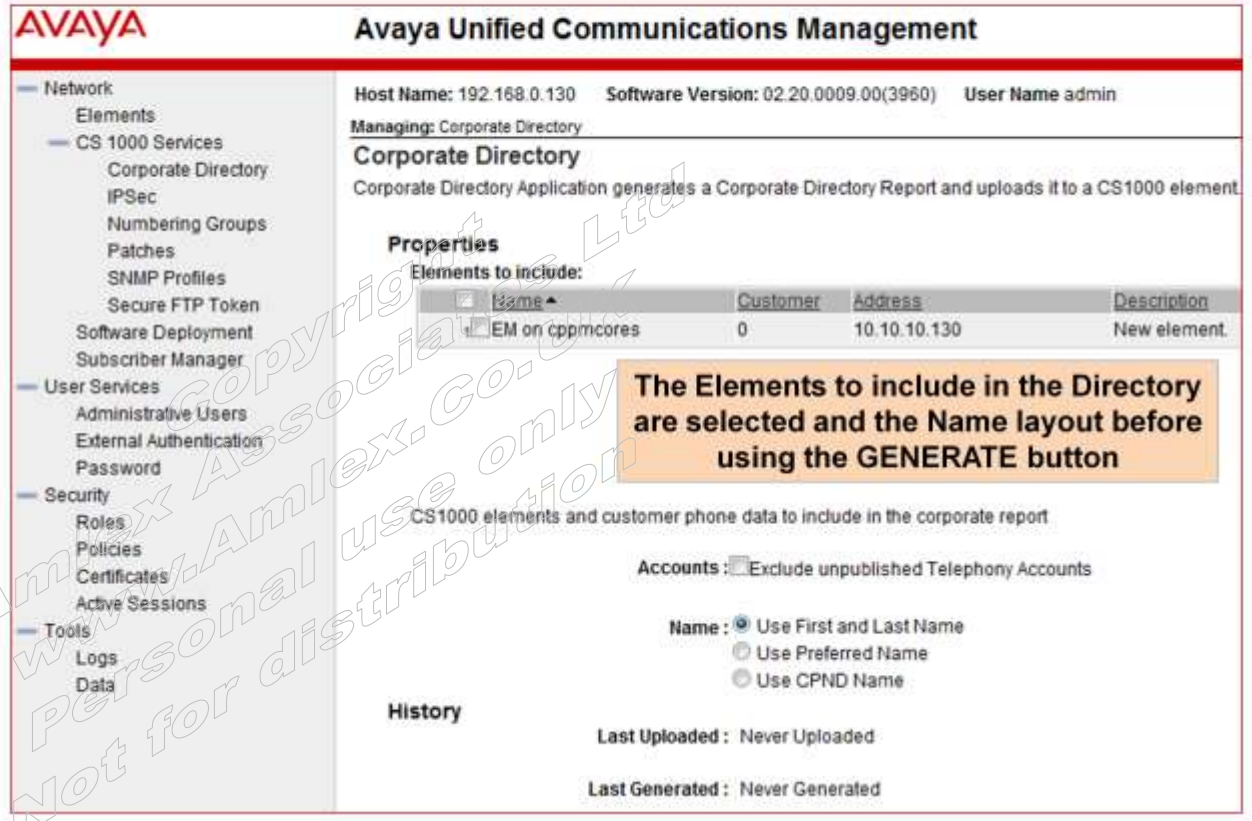
Corporate Directory

Once Subscriber Manager is populated generation of the Corporate Directory is possible.

As you can see in the example shown the elements to include in the Directory report are selected using the tick box and then the name order for generation.

Unpublished accounts can be excluded from the directory as required by selecting the appropriate option .

Finally the report is created using the **GENERATE** button .



178

Amlex Copyright www.Amlex.Associates Ltd Personal use only Not for distribution

Notes

_____

_____

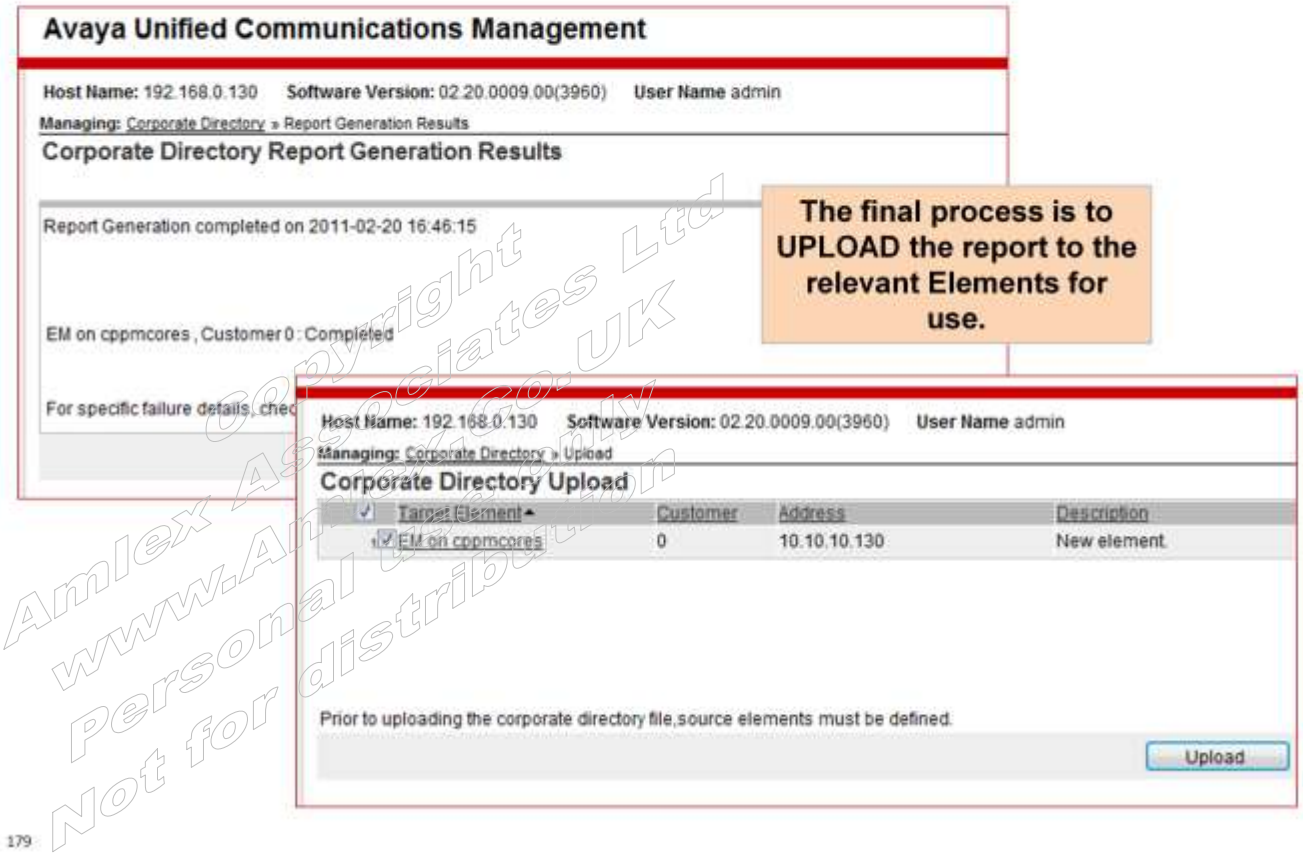
_____

_____

Corporate Directory

Once the report is generated all that is required is to upload it to the relevant elements for use.

Remember that Sets will need the correct class of service (CRPA) to use the corporate directory.


Avaya Unified Communications Management
Host Name: 192.168.0.130 Software Version: 02.20.0009.00(3960) User Name admin
Managing: Corporate Directory » Report Generation Results
Corporate Directory Report Generation Results
Report Generation completed on 2011-02-20 16:46:15
EM on cppmcores , Customer 0 : Completed
For specific failure details, chec
The final process is to UPLOAD the report to the relevant Elements for use.
Host Name: 192.168.0.130 Software Version: 02.20.0009.00(3960) User Name admin
Managing: Corporate Directory » Upload
Corporate Directory Upload
Target Element
Customer
Address
Description
EM on cppmcores
0
10.10.10.130
New element
Prior to uploading the corporate directory file,source elements must be defined.
Upload

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

179

Notes

_____

_____

_____

_____

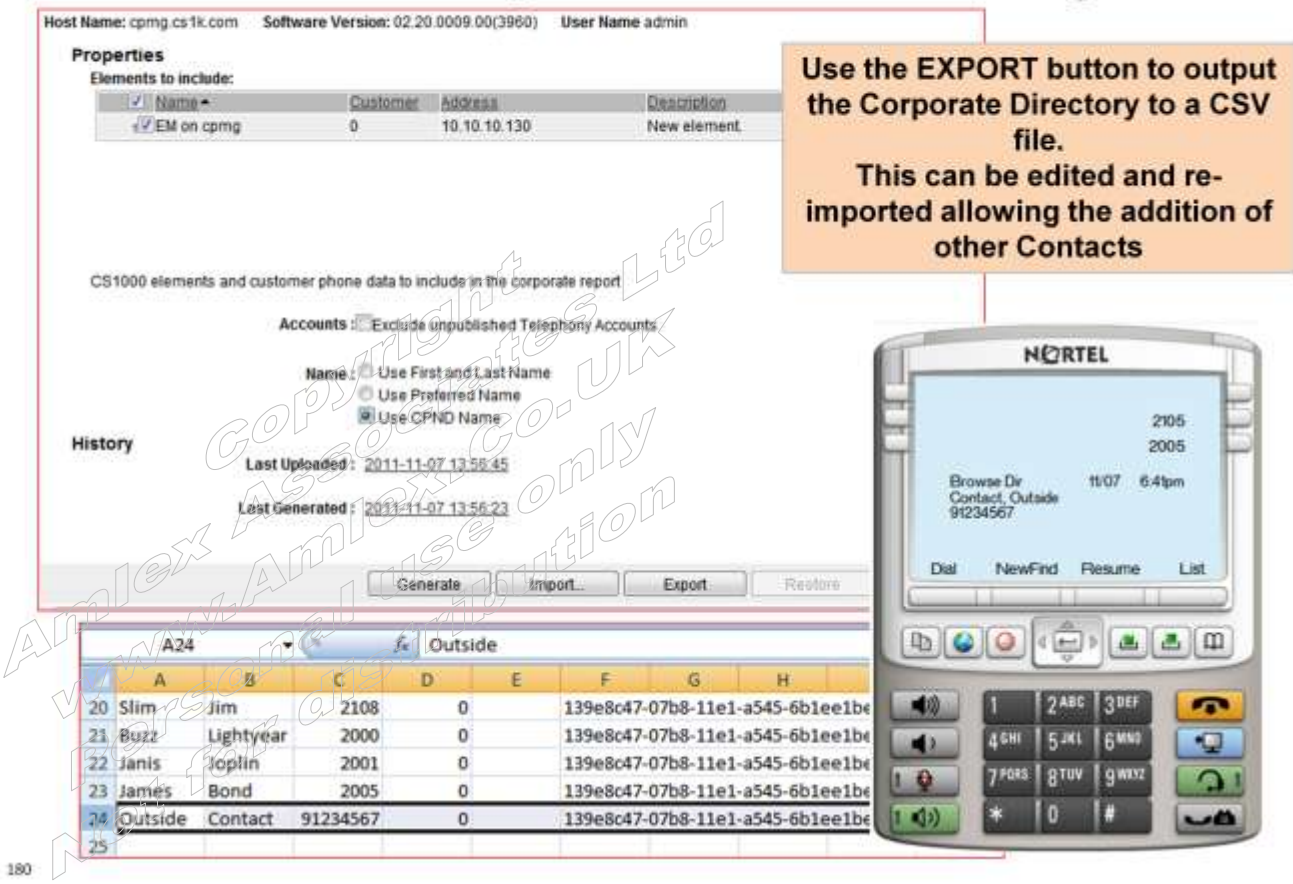
Copyright Amlex Associates Ltd

Edit Corporate Directory

Additions can be made to the Corporate directory by using the **EXPORT** button to create a CSV file of the entries called M1CorporateDirectoryReport.

This can be edited using Excel or similar but be sure to include the System ID number in any lines added.

Once the file is edited and saved use the **IMPORT** and **UPLOAD** buttons to update the stored Corporate Directory.


Host Name: cpmg.cs1k.com Software Version: 02.20.0009.00(3960) User Name admin
Properties
Elements to include:
Name Customer Address Description
EM on cpmg 0 10.10.10.130 New element.
Use the EXPORT button to output the Corporate Directory to a CSV file.
This can be edited and re-imported allowing the addition of other Contacts
CS1000 elements and customer phone data to include in the corporate report
Accounts : Exclude unpublished Telephony Accounts
Name : Use First and Last Name
Use Preferred Name
Use CPND Name
History
Last Uploaded : 2011-11-07 13:56:45
Last Generated : 2011-11-07 13:56:23
Generate
Import..
Export
Restore
A24
Outside
A B C D E F G H
20 Slim Jim 2108 0 139e8c47-07b8-11e1-a545-6b1ee1be
21 Buzz Lightyear 2000 0 139e8c47-07b8-11e1-a545-6b1ee1be
22 Janis Joplin 2001 0 139e8c47-07b8-11e1-a545-6b1ee1be
23 James Bond 2005 0 139e8c47-07b8-11e1-a545-6b1ee1be
24 Outside Contact 91234567 0 139e8c47-07b8-11e1-a545-6b1ee1be
25
180
NORTEL
2105
2005
Browse Dir
Contact, Outside
91234567
11/07 6:41pm
Dial NewFind Resume List

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Manually add Corporate Directory

The Corporate Directory can be created manually within Excel or a similar programme as shown here.

NOTE:- It is important to have the fourth column D as shown or the file will not be recognised when uploaded to the Call Server.

Once the names and numbers (again including external numbers) have been recorded in the spreadsheet they must be sorted into Alphabetical order to ensure they are found correctly within the Corporate Directory search function on the phones.

NOTE:- the storage of the Corporate Directory on the Call Server is very simplistic and when a search is done the pointer in the file simply moves to the first instance of the searched for letters. Thus with an unsorted file spurious results will occur.

Once the file is sorted it must be saved as a comma separated values (CSV) file using the name CpDir0.csv.

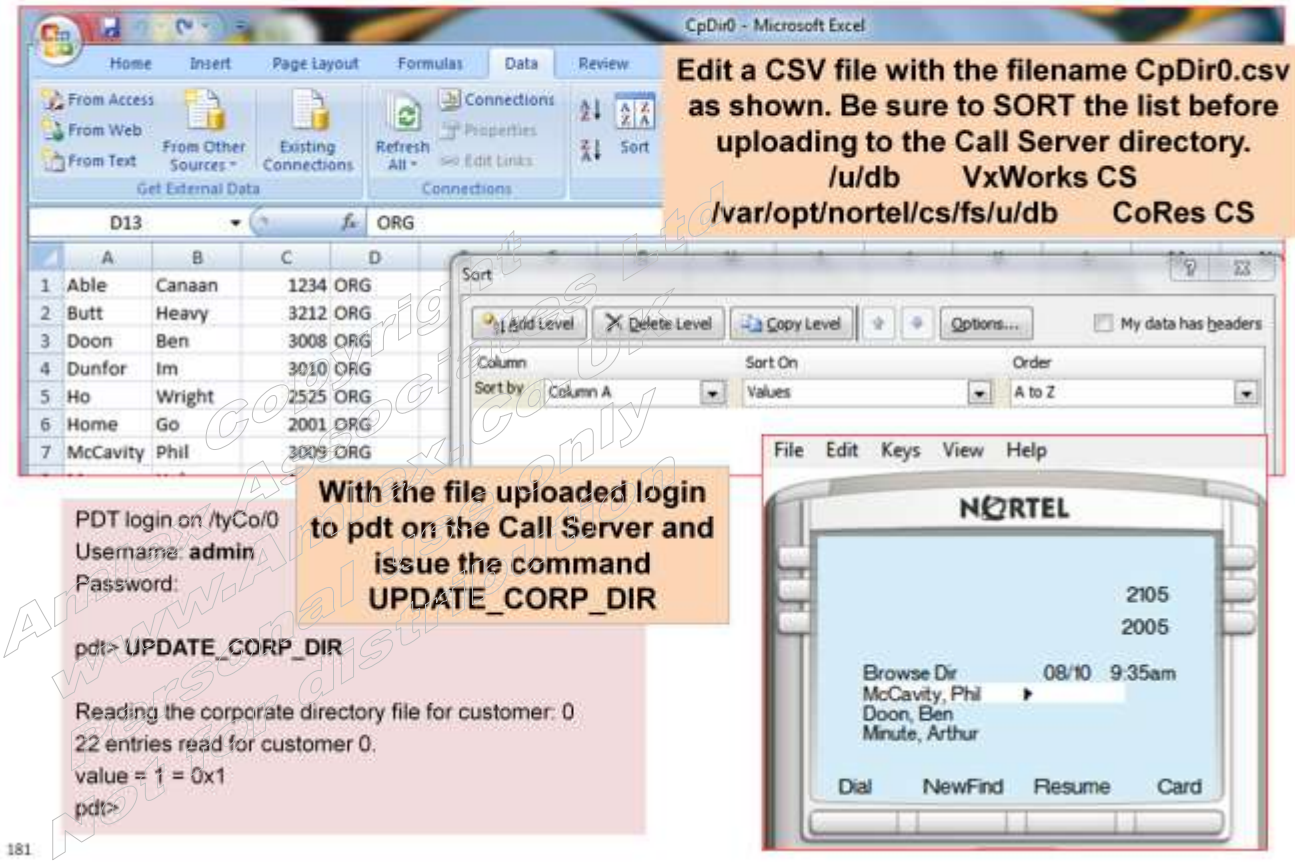
This is then uploaded to the Call Server with Filezilla or similar into the location:-

VxWorks CS /u/db
CoRes CS /var/opt/nortel/cs/fs/u/db

Then from the PDT command line issue the command :-

UPDATE_CORP_DIR

Which will load the names into the Corporate Directory storage space.


CpDir0 - Microsoft Excel
Edit a CSV file with the filename CpDir0.csv as shown. Be sure to SORT the list before uploading to the Call Server directory.
/u/db VxWorks CS
/var/opt/nortel/cs/fs/u/db CoRes CS
With the file uploaded login to pdt on the Call Server and issue the command UPDATE_CORP_DIR
PDT login on /tyCo/0
Username: admin
Password:
pdt> UPDATE_CORP_DIR
Reading the corporate directory file for customer: 0
22 entries read for customer 0.
value = 1 = 0x1
pdt>
NORTEL
2105
2005
Browse Dir 08/10 9:35am
McCavity, Phil
Doon, Ben
Minute, Arthur
Dial NewFind Resume Card

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

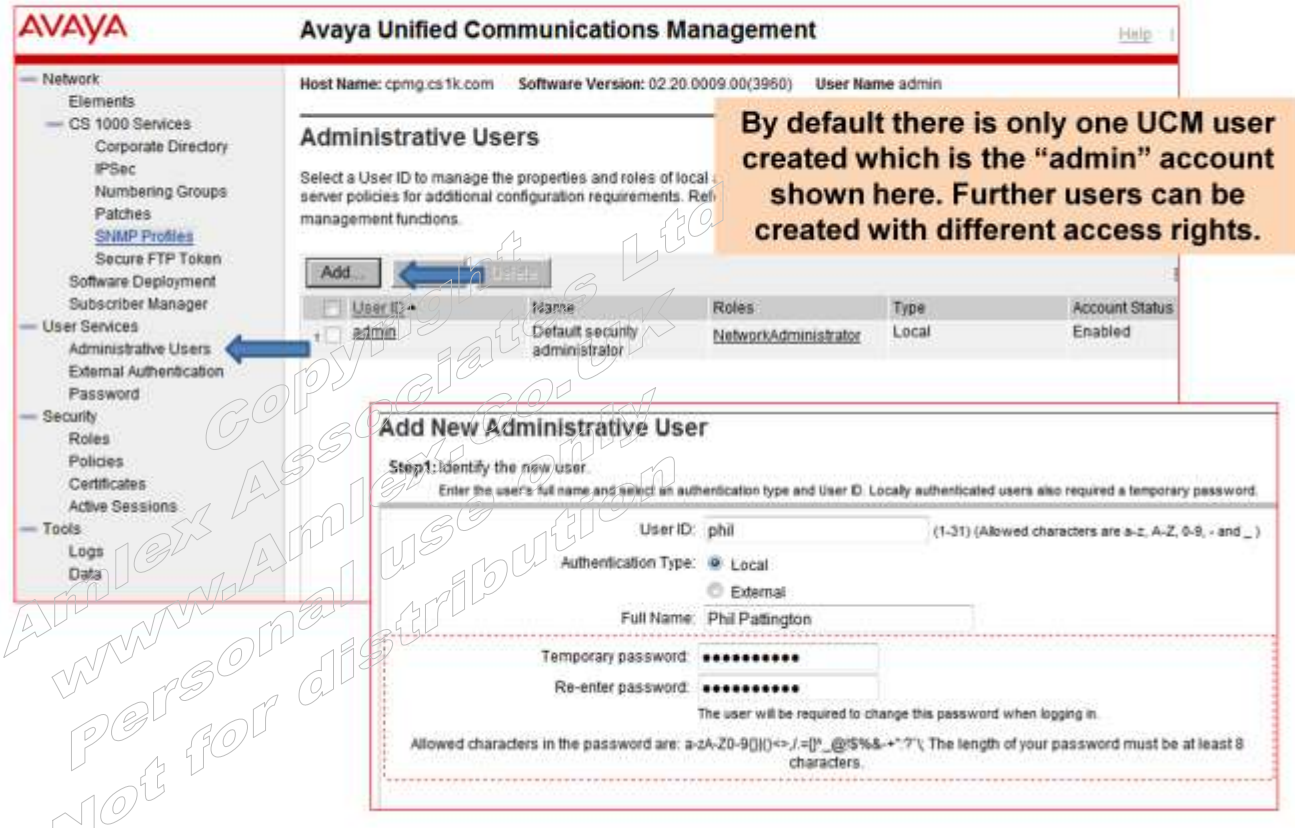
16. UCM Users & Roles

Initially the UCM has only one user which is the “admin” account. This is a fully privileged account and should be reserved for use by those that need it.

Additional users should be created on the UCM to allow others to login whilst controlling their access to the system.

To add a new user select the ADMINISTRATIVE USERS option under USER SERVICES, then click on the ADD button . You need to add the new user name and the Full name and a Temporary Password which will be changed at the first login before proceeding.

NOTE :-
UCM usernames and passwords will allow you to login to the Linux base but are not strictly Linux users. The two Linux accounts on each Linux server are “root” and “admin2” (Not the same as the “admin2” user in the overlays).



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

182

Notes

_____

_____

_____

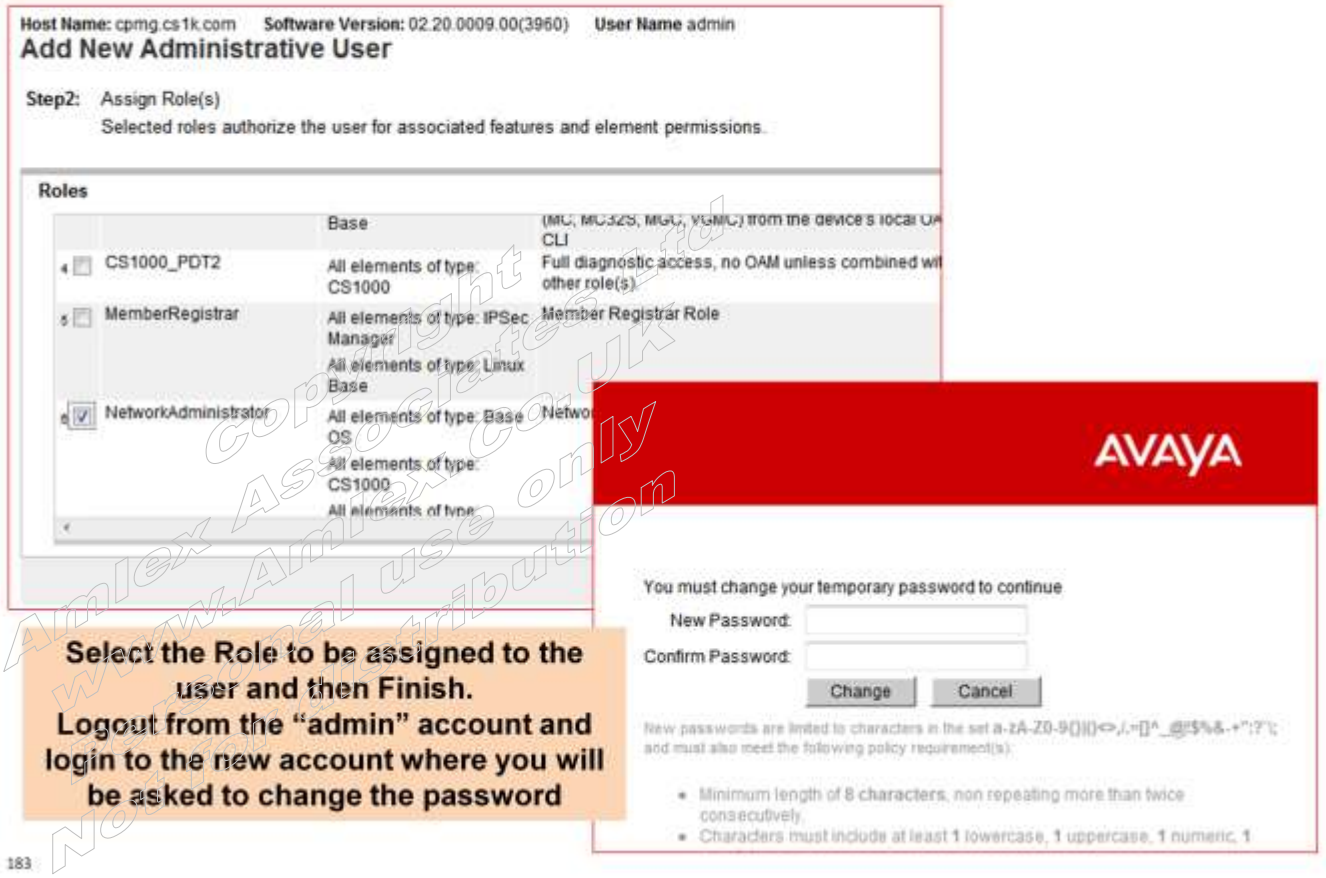
_____

Add Predefined Role

Once the user is initially created the Role can now be assigned. This defines the access the user will have to the system.

There are a number of pre-defined roles on the system covering the different areas that a user may be allocated to look after such as CS1000_Admin1 & CS1000_Admin2. These are allocated to the user to complete configuration.

Once the new user is created the first time the account is used the system will prompt for the Temporary password to be changed before logging onto the system.


Host Name: cpmg.cs1k.com Software Version: 02.20.0009.00(3960) User Name admin
Add New Administrative User
Step2: Assign Role(s)
Selected roles authorize the user for associated features and element permissions.
Roles
CS1000_PDT2
MemberRegistrar
NetworkAdministrator
Member Registrar Role
AVAYA
You must change your temporary password to continue
New Password:
Confirm Password:
Change
Cancel
Select the Role to be assigned to the user and then Finish.
Logout from the "admin" account and login to the new account where you will be asked to change the password
183

Notes

_____

_____

_____

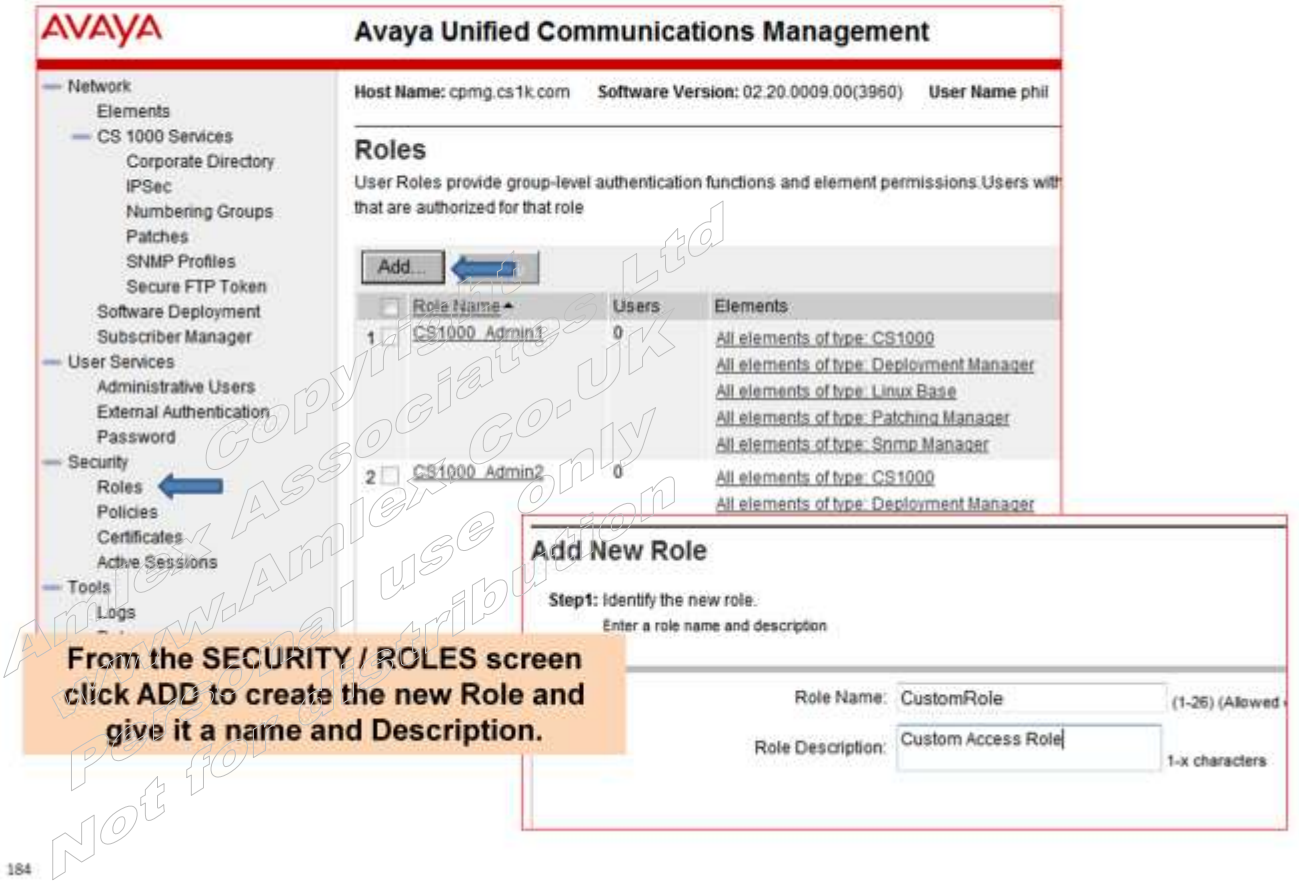
_____

Copyright Amlex Associates Ltd

Create a Custom Role

If the standard roles do not cover the access required on the system it is possible to create a Custom Role which can then be allocated to the user. A simple case is that of restricting a user to only one system on the UCM.

Similar to the user creation the new role is ADDed and saved before selecting the specific tasks and access rights.



Notes

_____

_____

_____

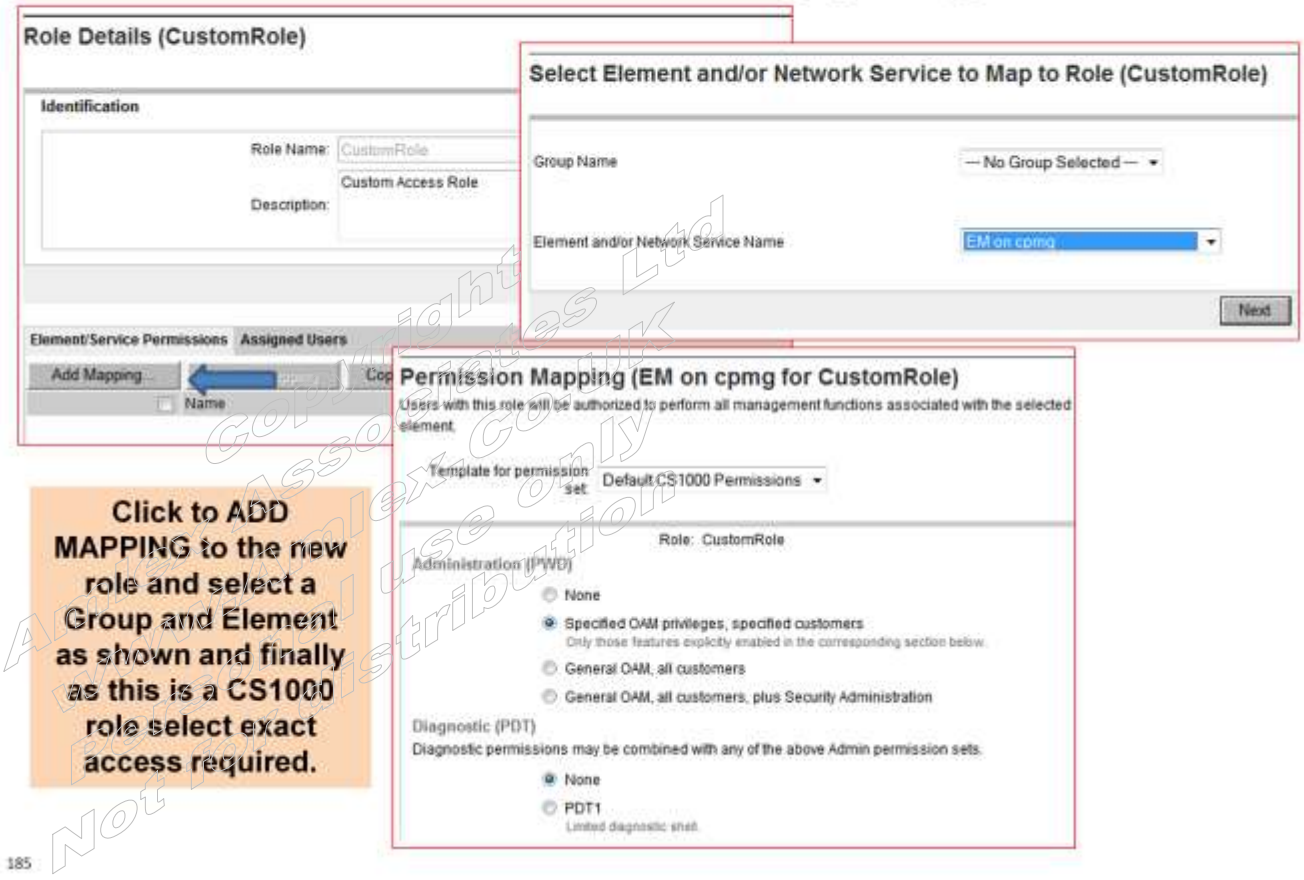
_____

Copyright Amlex Associates Ltd

Add Role Mapping

Using the ADD MAPPING button you are presented with the options for GROUP and ELEMENT or NETWORK SERVICE. Here we have selected the EM on cpmg i.e. We are restricting access to just the system “cpmg”.

After this we can add very specific access rights similar to a Limited Access Password in the overlays.


Role Details (CustomRole)
Identification
Role Name: CustomRole
Description: Custom Access Role
Element/Service Permissions
Assigned Users
Add Mapping...
Name
Select Element and/or Network Service to Map to Role (CustomRole)
Group Name
— No Group Selected —
Element and/or Network Service Name
EM on cpmg
Next
Permission Mapping (EM on cpmg for CustomRole)
Users with this role will be authorized to perform all management functions associated with the selected element.
Template for permission set: Default CS1000 Permissions
Role: CustomRole
Administration (PWD)
None
Specified OAM privileges, specified customers
Only those features explicitly enabled in the corresponding section below.
General OAM, all customers
General OAM, all customers, plus Security Administration
Diagnostic (PDT)
Diagnostic permissions may be combined with any of the above Admin permission sets.
None
PDT1
Limited diagnostic shell
Click to ADD MAPPING to the new role and select a Group and Element as shown and finally as this is a CS1000 role select exact access required.
185

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

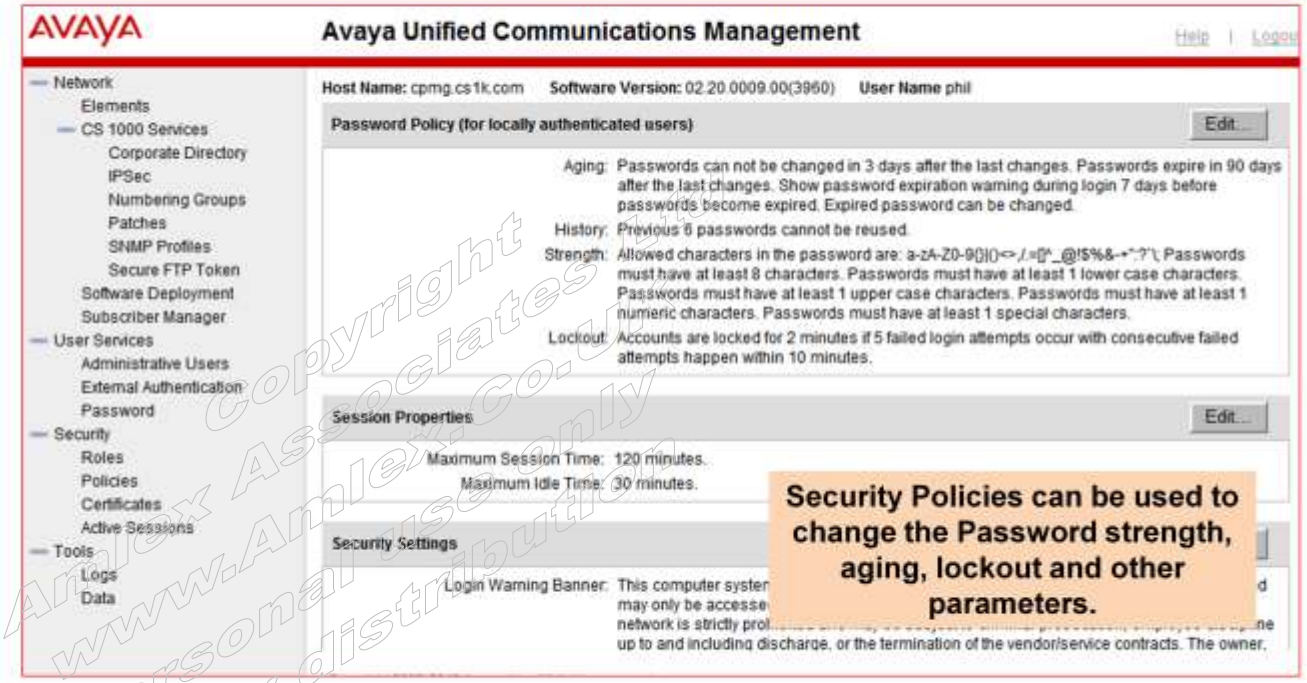
Security Policies

The password on the UCM are complex by default and require four different character types at least, also passwords must exist a minimum of 3 days before they can be changed and also they will expire after 90 days.

These security settings are accessed via the SECURITY / POLICIES menu option. Here you can increase or relay password strength and aging etc.

In addition there are settings for the Maximum session duration and the maximum idle time as well as the login banner message.

Think carefully before reducing any of the system security settings.


AVAYA
Avaya Unified Communications Management
Help | Logou
Network
Elements
CS 1000 Services
Corporate Directory
IPSec
Numbering Groups
Patches
SNMP Profiles
Secure FTP Token
Software Deployment
Subscriber Manager
User Services
Administrative Users
External Authentication
Password
Security
Roles
Policies
Certificates
Active Sessions
Tools
Logs
Data
Host Name: cpmg.cs1k.com Software Version: 02.20.0009.00(3960) User Name phil
Password Policy (for locally authenticated users)
Edit...
Aging: Passwords can not be changed in 3 days after the last changes. Passwords expire in 90 days after the last changes. Show password expiration warning during login 7 days before passwords become expired. Expired password can be changed.
History: Previous 6 passwords cannot be reused.
Strength: Allowed characters in the password are: a-zA-Z0-9{}[]()<>,/.=@^_@!$%&-+*:?'\ Passwords must have at least 8 characters. Passwords must have at least 1 lower case characters. Passwords must have at least 1 upper case characters. Passwords must have at least 1 numeric characters. Passwords must have at least 1 special characters.
Lockout: Accounts are locked for 2 minutes if 5 failed login attempts occur with consecutive failed attempts happen within 10 minutes.
Session Properties
Edit...
Maximum Session Time: 120 minutes.
Maximum Idle Time: 30 minutes.
Security Settings
Login Warning Banner:
Security Policies can be used to change the Password strength, aging, lockout and other parameters.

Amlex Associates Co.Uk Copyright www.Amlex.co.uk Personal use only Not for distribution

186

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Exercise

- Create a new Network Administrator user
- Create a new CS1000 Admin2 user
- Create a Custom Role to restrict access
  - Limit to certain Overlays
  - Assign Custom role to a new user
- Change the system Security Policies
  - Increase the aging time
  - Reduce the number of passwords remembered
  - Change the complexity of the passwords required
  - Change the Login Banner
  - Increase the Maximum Session Time

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

187

Notes

_____

_____

_____

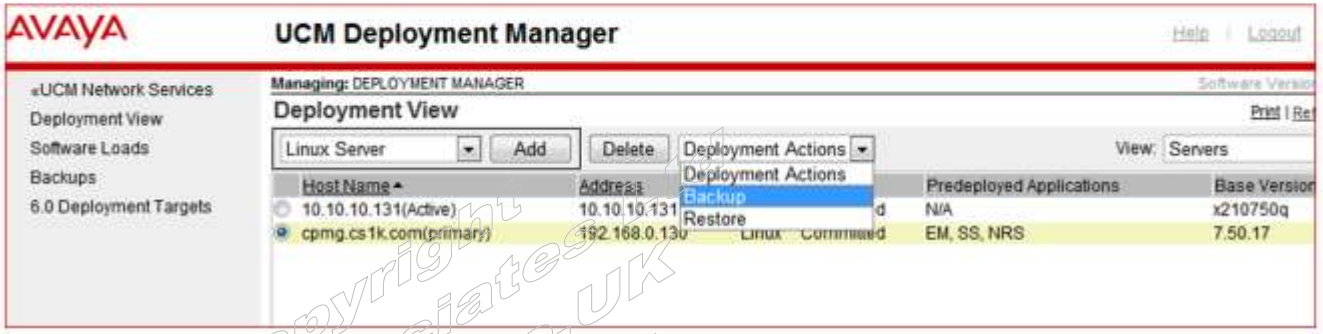
_____

17. UCM Deployment Backup

With the introduction or Release 6 and the UCM, comes a new option for backup of the whole system not just the call server.

The UCM backup can be regarded as a disaster recovery option in as much as it saves the UCM environment including the Certificates and Authorisation information. On a CoRes call server it will also save the last EDD backup and NRS if deployed on the same Linux server.

To create a UCM deployment backup select the option **CS1000 SERVICES / SOFTWARE DEPLOYMENT**. After selecting the server to backup via the radio button use the drop down menu to select **BACKUP** which will display the backup page and offer you the option of saving the backup to the Deployment Server itself (Primary UCM) or an SFTP server.



Managing: DEPLOYMENT MANAGER
Backup
Host name: cpmg
Type: CPMG32
Server status: Deployed
Deployed version: 7.50.17-00
Applications: NRS+SS, EM
Current operation status: None
Select backup location: Deployment Server
Start Backup
A UCM backup contains the settings information for the UCM Linux server.
A backup of the Primary UCM carries the Certificate information and so is a requisite to restore a failed server

188

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

When the backup is executed it will save the relevant information and then use TAR and GUNZIP to compress it into a single file which is named by combining the server name with the date and time the backup was executed.

The backup is saved to the directory :-

/var/opt/nortel/deployment/deployed/<servername>/backup

and can be downloaded for storage on another system if required using an SFTP client.

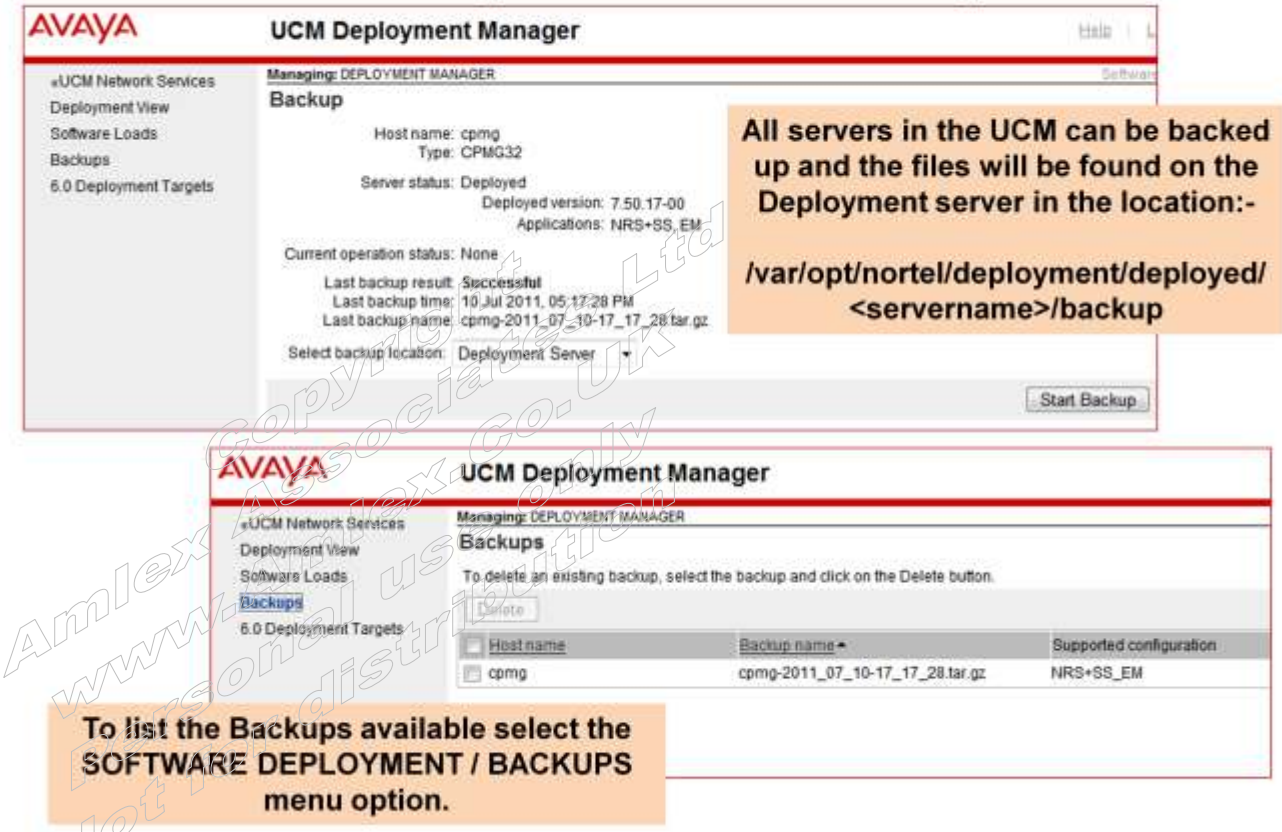
Clicking on the BACKUPS menu option will show a list of all the backups held on the deployment server.

In this example you can see the backup of the one server.

NOTE:-
On upgraded CPPM cards which still have the 40Gb hard drive be careful of the number of backups stored as disk space can be an issue.

UCM backups store the patches and service packs applied to them and thus the size can escalate.

Completed Backup



Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

189

Notes

_____

_____

_____

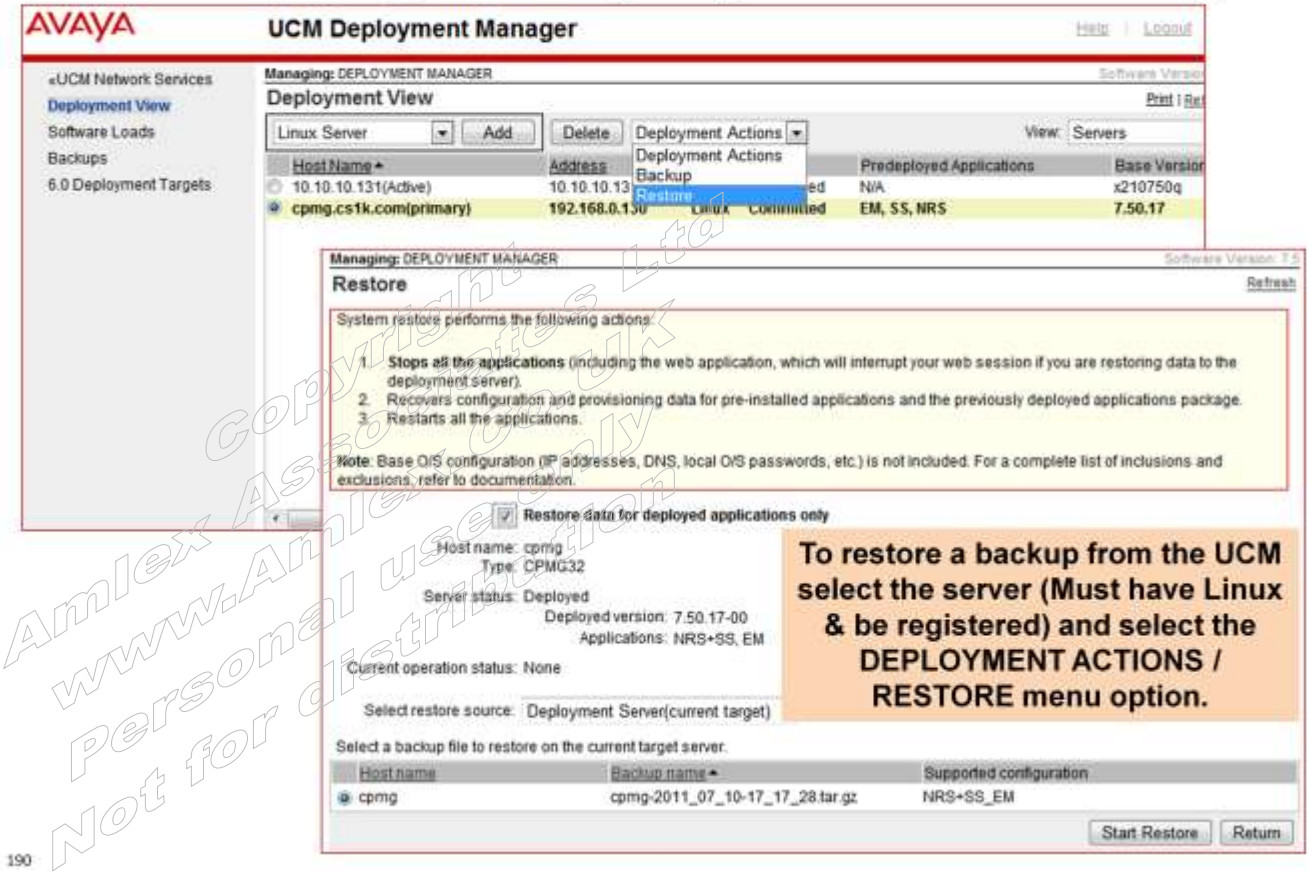
_____

Restoring a Deployment Backup

To restore a Deployment Backup select the server to restore and click on the **RESTORE** button.

The system will then warn you of what will be restored and what will not. Note that this type of restore does not include the Base O/S information.

You are then asked to select the backup to restore before proceeding with the actual restore.



Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

The full system backup can also be created using the command line, this option has some other benefits in that it can be scheduled.

The command is:-
sysbackup
Usage:
sysbackup -r|-s|-b|-c|[--help]
Options:
-r remove backup task from schedule
-s show backup task schedule setting
-b execute one-time backup
-c setup a backup schedule

The backup maybe sent to either a USB stick or SFTP server and this is selected after the command is issued. The backup created can be used as a complete system restore (including CoRes CS & NRS).

This is done by initiating a Linux install and using option 2 or 3 as the backup location.

Once the Linux has been restored the application file (.nai) is loaded and the applications re-deployed. At this point the system will prompt to use the backed up data.

USB Backup & Restore

- Backup - $sysbackup –b
  - Choose USB or SFTP option
  - If CoRes EDD first
  - Can use UCM backup and copy to USB
- Restore
  - Boot server to installer
    - F on CPPM or boot with DVD on COTS
    - Choose option 2 or 3 to restore from USB or SFTP
    - After reboot Element list & UCM back
  - Add software load - .nai file
  - Deploy server using backup information
    - Appears as an UPGRADE
    - Requests Keycode file
    - Use EXISTING DATABASE

191

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Notes
_____
_____
_____
_____

18. Linux CLI

Use "admin2" for CLI access

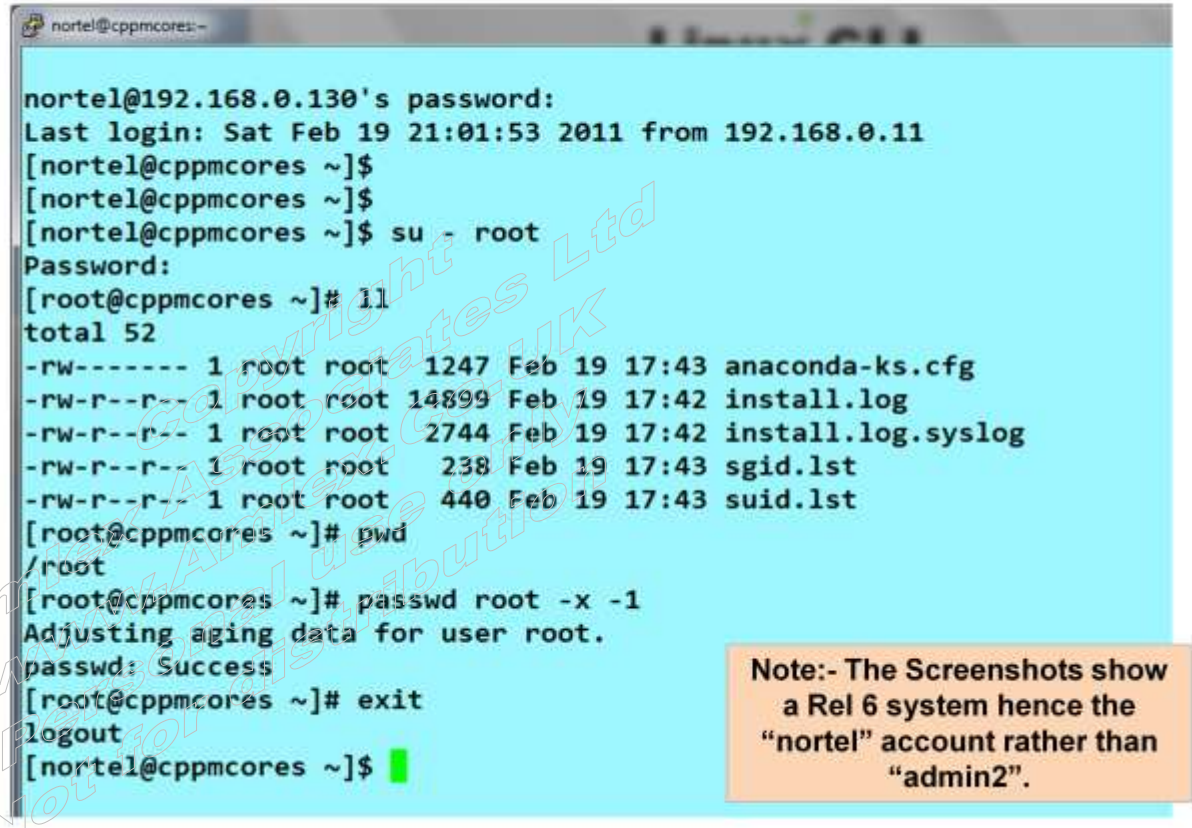
logout/exit/<ctrl>d % Exits session
<ctrl>c % To break out if locked
su "uname" % Switch User . Add –l to use login directory
pwd % Show current Directory
ls % List the current directory in short format
ll % List the current directory in long format

tail <logfile> % Display 10 (default) most recent entries in a log file
tail –100 <logfile> % Display 100 most recent entries in a log file
tail –f <logfile> % Live monitor events as they are written to a log file
tail –f <logfile> | grep <string> Live monitor events as they are written to log file and only display lines containing <string>

Stop ageing of LINUX passwords.
Login as root
passwd "Username" –x -1
e.g. > **passwd root –x -1**

mount /dev/sda1 /<temp dir name> -t vfat % Mounts a usb stick onto a temporary directory
umount /dev/sda1 % Unmount the usb stick before removing

networkconfig Config IP Addresses
datetimeconfig Set date and time


nortel@cppmcores:~
nortel@192.168.0.130's password:
Last login: Sat Feb 19 21:01:53 2011 from 192.168.0.11
[nortel@cppmcores ~]$
[nortel@cppmcores ~]$
[nortel@cppmcores ~]$ su - root
Password:
[root@cppmcores ~]# ll
total 52
-rw------- 1 root root 1247 Feb 19 17:43 anaconda-ks.cfg
-rw-r--r-- 1 root root 14899 Feb 19 17:42 install.log
-rw-r--r-- 1 root root 2744 Feb 19 17:42 install.log.syslog
-rw-r--r-- 1 root root 238 Feb 19 17:43 sgid.lst
-rw-r--r-- 1 root root 440 Feb 19 17:43 suid.lst
[root@cppmcores ~]# pwd
/root
[root@cppmcores ~]# passwd root -x -1
Adjusting aging data for user root.
passwd: Success
[root@cppmcores ~]# exit
logout
[nortel@cppmcores ~]$

Note:- The Screenshots show a Rel 6 system hence the "nortel" account rather than "admin2".

192

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

cd /dir/dir % Change directory to the fully qualified path
cd dir/dir % Change directory to the path relative to the current working directory
cd .. % Change to the parent directory

man <cmd> % Open online manual for command specified

cat <filename> % Print entire contents of a file from start to finish

find / -name *.log % Print the pathname to any file ending in .log (works best when logged in as root)

Up arrow %Recalls previous commands
Tab key % Auto complete filenames eg cd /tm <tabkey> will change directory to /tmp as there is no other directories or files under root beginning with tm.

mkdir <dir name> % Create a directory

rmdir <dir name> % Delete a directory
more <filename> % Print the contents of a file (advance a line at a time with CR key or a page at a time with SPACE key.

df % Disk space on devices.

cp % Copy a file or files

halt % Stops Linux in a controlled manner better than just turning off power, login as root first.

Linux CLI

Copyright Amlex Associates Ltd
Not for distribution
General use only

193

Notes

_____

_____

_____

_____

APPSTART & TOP commands

The command to use to view the status of the Nortel applications is:-

appstart status

It can also be used to stop start or restart any of the Nortel applications and removes the need to restart the whole machine. The command:-

appstart restart

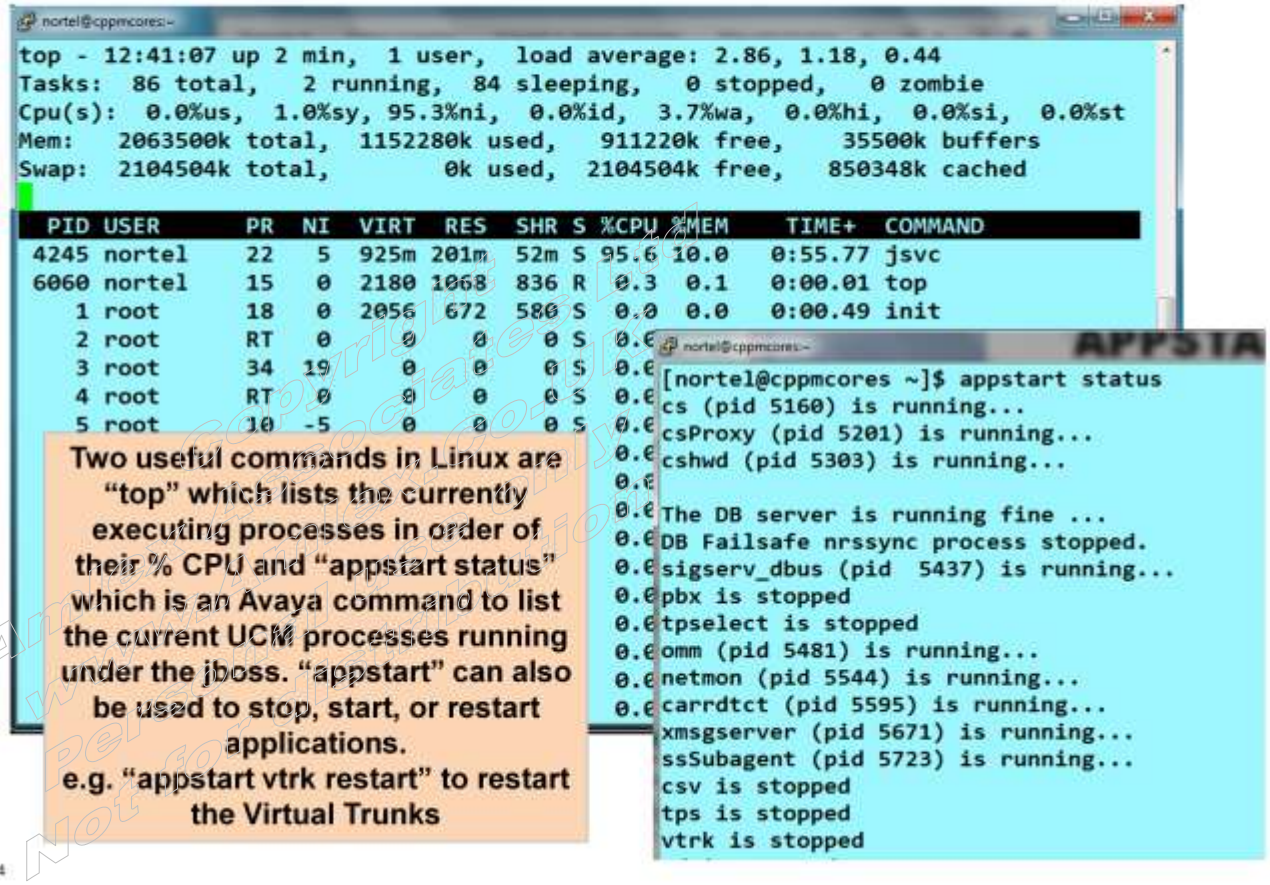
will restart all of the Nortel applications running whereas:-

appstart vtrk restart
will just restart the virtual trunk module.

The command:-

top

is useful for gauging how busy the system is as it shows the top (busiest) processes and how much CPU and Memory they are consuming.


top - 12:41:07 up 2 min, 1 user, load average: 2.86, 1.18, 0.44
Tasks: 86 total, 2 running, 84 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 1.0%sy, 95.3%ni, 0.0%id, 3.7%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 2063500k total, 1152280k used, 911220k free, 35500k buffers
Swap: 2104504k total, 0k used, 2104504k free, 850348k cached
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
4245 nortel 22 5 925m 201m 52m S 95.6 10.0 0:55.77 jsvc
6060 nortel 15 0 2180 1068 836 R 0.3 0.1 0:00.01 top
1 root 18 0 2056 672 580 S 0.0 0.0 0:00.49 init
2 root RT 0 0 0 0 S
3 root 34 19 0 0 0 S
4 root RT 0 0 0 0 S
5 root 10 -5 0 0 0 S
[nortel@cppmcores ~]$ appstart status
cs (pid 5160) is running...
csProxy (pid 5201) is running...
cshwd (pid 5303) is running...
The DB server is running fine ...
DB Failsafe nrssync process stopped.
sigserv_dbus (pid 5437) is running...
pbx is stopped
tpselect is stopped
omm (pid 5481) is running...
netmon (pid 5544) is running...
carrdtct (pid 5595) is running...
xmsgserver (pid 5671) is running...
ssSubagent (pid 5723) is running...
csv is stopped
tps is stopped
vtrk is stopped
Two useful commands in Linux are "top" which lists the currently executing processes in order of their % CPU and "appstart status" which is an Avaya command to list the current UCM processes running under the jboss. "appstart" can also be used to stop, start, or restart applications.
e.g. "appstart vtrk restart" to restart the Virtual Trunks
194

Notes

_____

_____

_____

_____

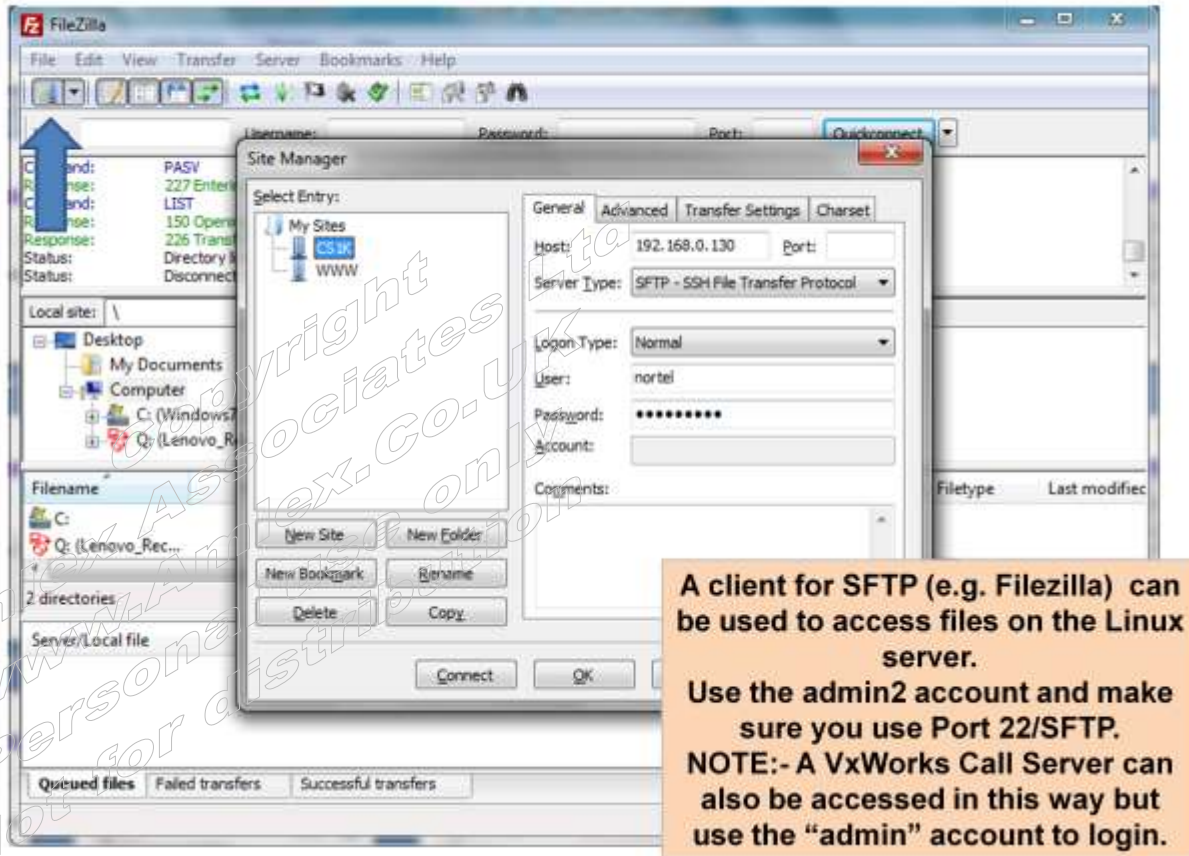
Copyright Amlex Associates Ltd

Secure FTP Access (SFTP)

Using a Secure File Transfer Protocol client it is easy to connect to the Linux server and access the file structure. Shown here is the Filezilla client. Use the “nortel” account to login as this will allow the best access to files and directories.

To set up a connection click on the **SITE MANAGER** icon arrowed which will open the dialogue shown. Add the host IP address to connect to and select the server type SFTP.

The logon type is NORMAL and add the account to use for login in this case “nortel” as its Rel 6 but on Rel 7.5 systems “admin2”. When you connect you will be placed in the home directory for the login account i.e. /home/nortel .



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

195

Notes

_____

_____

_____

_____

Moving Files

Files can be dragged and dropped in either direction to move them on or off the server e.g. Backup to the PC, patch files to the Linux server.

Navigation is done either by clicking the Icons or by typing the location in the arrowed field.

File locations

Patch files need to be located in
/var/opt/nortel/patch

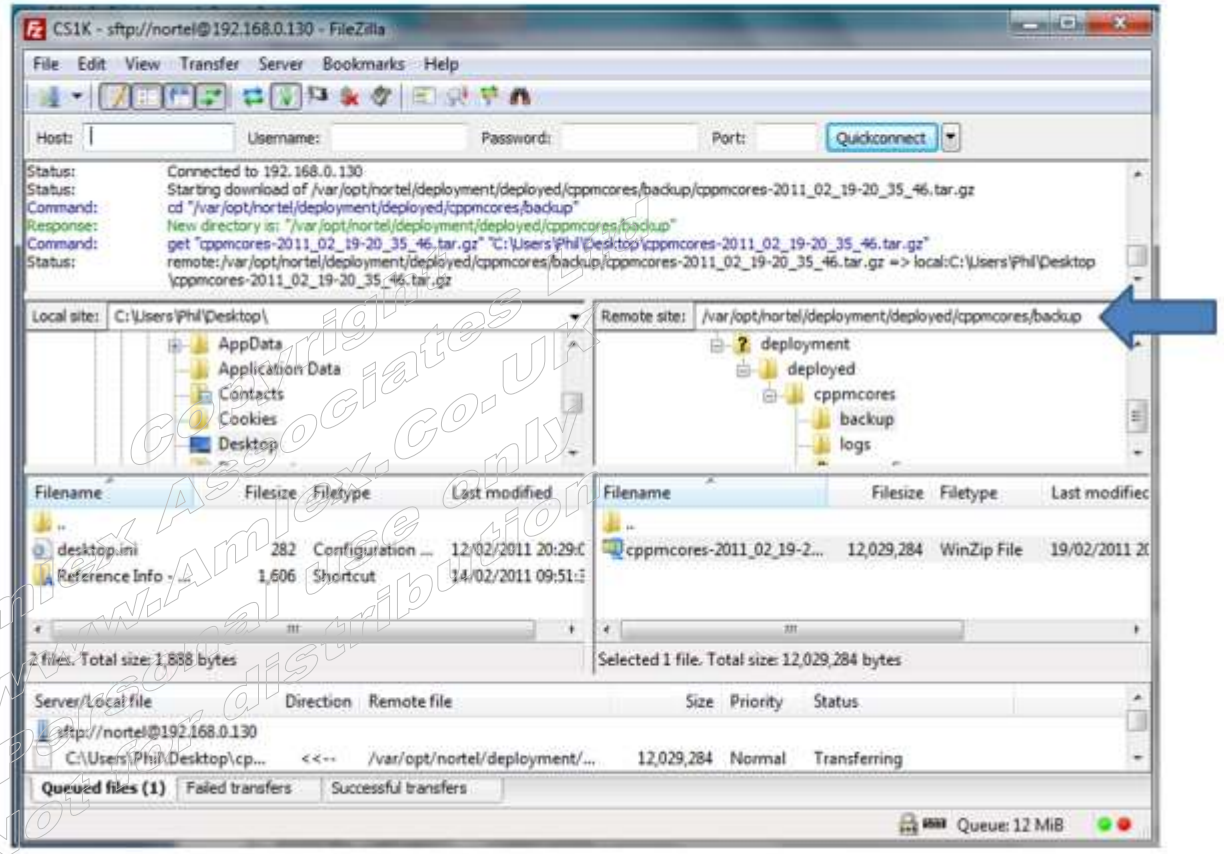
Application Log files are located in
/var/log/nortel

CPPM-Cores file system (/p /u /e) is located at
/var/opt/nortel/cs/fs

CS RPT log files are located in
/var/opt/nortel/cs/fs/e/rpt/
(use rdopen/rdtail in pdt to view)

DCH trace logs are located in
/var/opt/nortel/cs/fs/u/trace/dch.log

Deployment backup files
/var/opt/nortel/deployment/deployed/”sys name”/backup



Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution
Copyright

196

Notes

_____

_____

_____

_____

NOTE:- Avaya procedures may require certain Patches and Service Updates to be applied in a specific fashion.

Ensure you check any special instruction and notes pertaining to the patches to be installed.

19. Patching

- **Centralised Patching**
  - Linux Patching from Primary UCM
  - Remote Patching
  - Patches Linux Applications SS, Sub Mgr, NRS etc.
- **Local Patching**
  - Patching from Linux Base – Single server
- **Patching from Command line**
  - Patching using the command line commands
- **Call server Patching**
  - Adding Patches to the Call Server

197

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

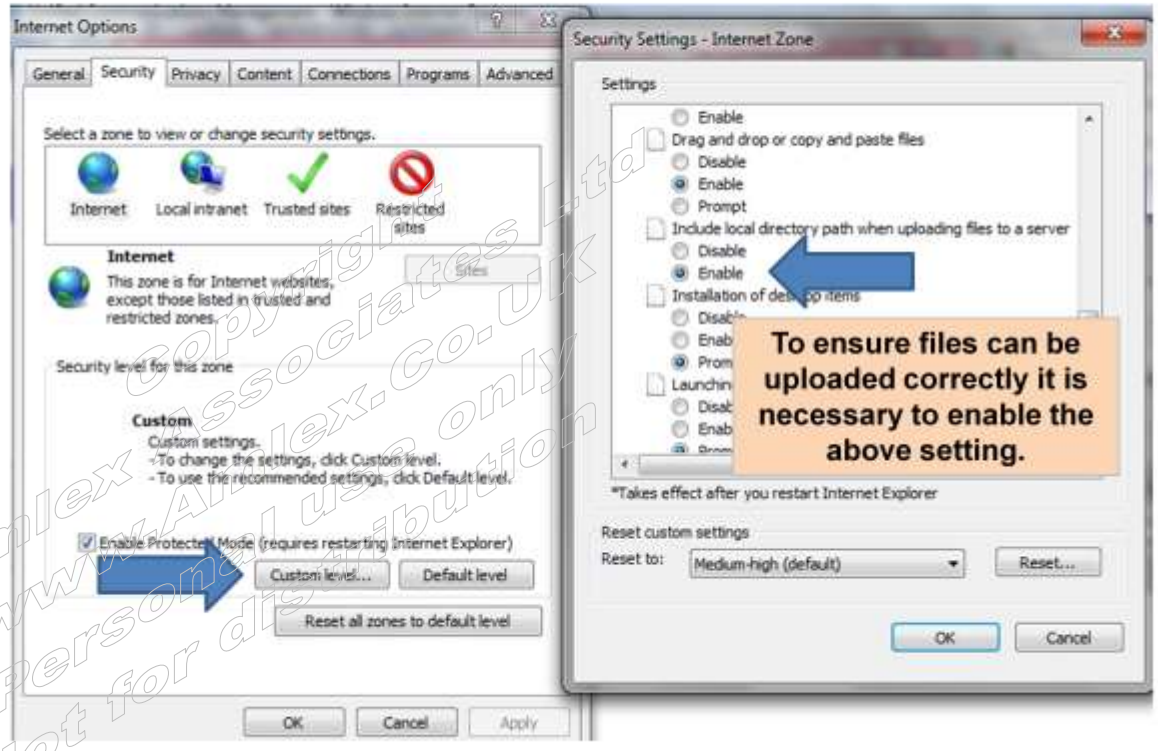
Issues with Internet Explorer 8

There are some issues with uploading of files from IE8 which makes patching difficult. To overcome these if you are using IE8 make sure you change the settings shown on your web browser.

Go to **INTERNET OPTIONS** under the **TOOLS** menu, select the **SECURITY** tab as shown and click to change the **CUSTOM LEVEL** for Internet.

This will give the options on the right where you need to change the option **INCLUDE LOCAL DIRECTORY PATH WHEN UPLOADING FILES TO SERVER** to **ENABLE**.

This should allow the correct upload of Patches and Service Packs to the UCM server for centralised Deployment.



198

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

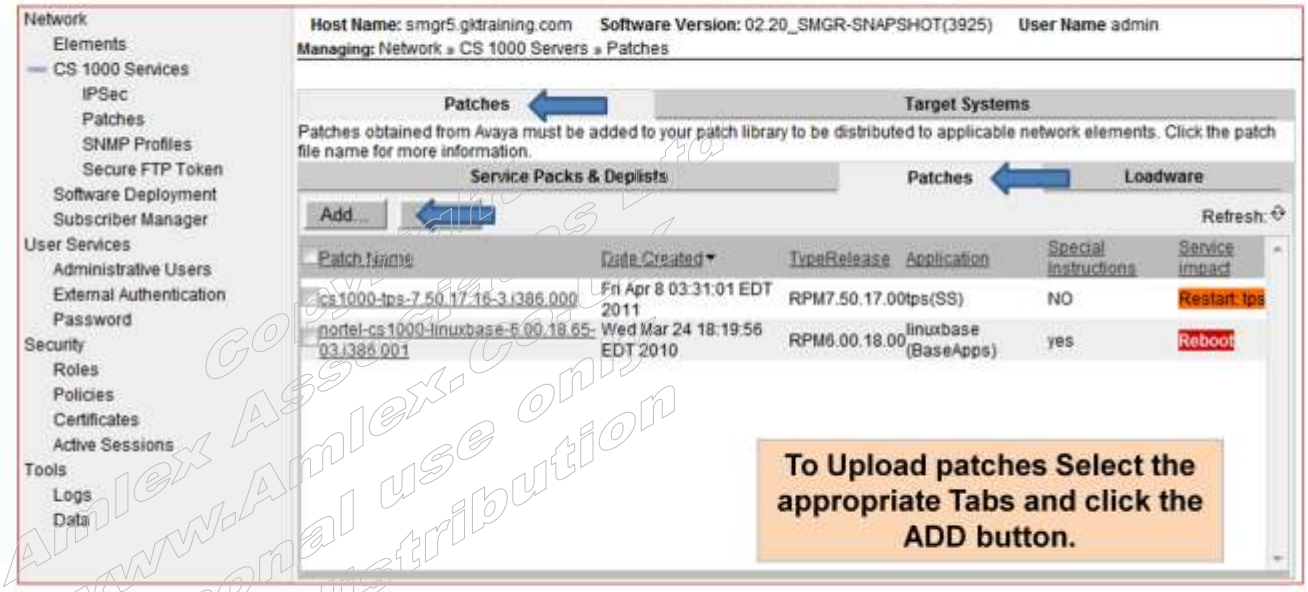
Centralised Patching

The benefit of Centralised Patching is that you only upload the patch once to the Primary UCM and then it can be deployed to all the Linux servers in the network.

The patching process is broadly the same on the Linux server for Individual Patches (sometimes called Service Updates) and Service Packs. However be sure to select the correct tab for the type of patch you are adding.

To add a patch or service pack use the **ADD** button shown, browse to the file required and **UPLOAD**.

Once the patches are on the Primary UCM they can be deployed to the network servers. However you must patch the Primary UCM before any other server.



199

Notes

_____

_____

_____

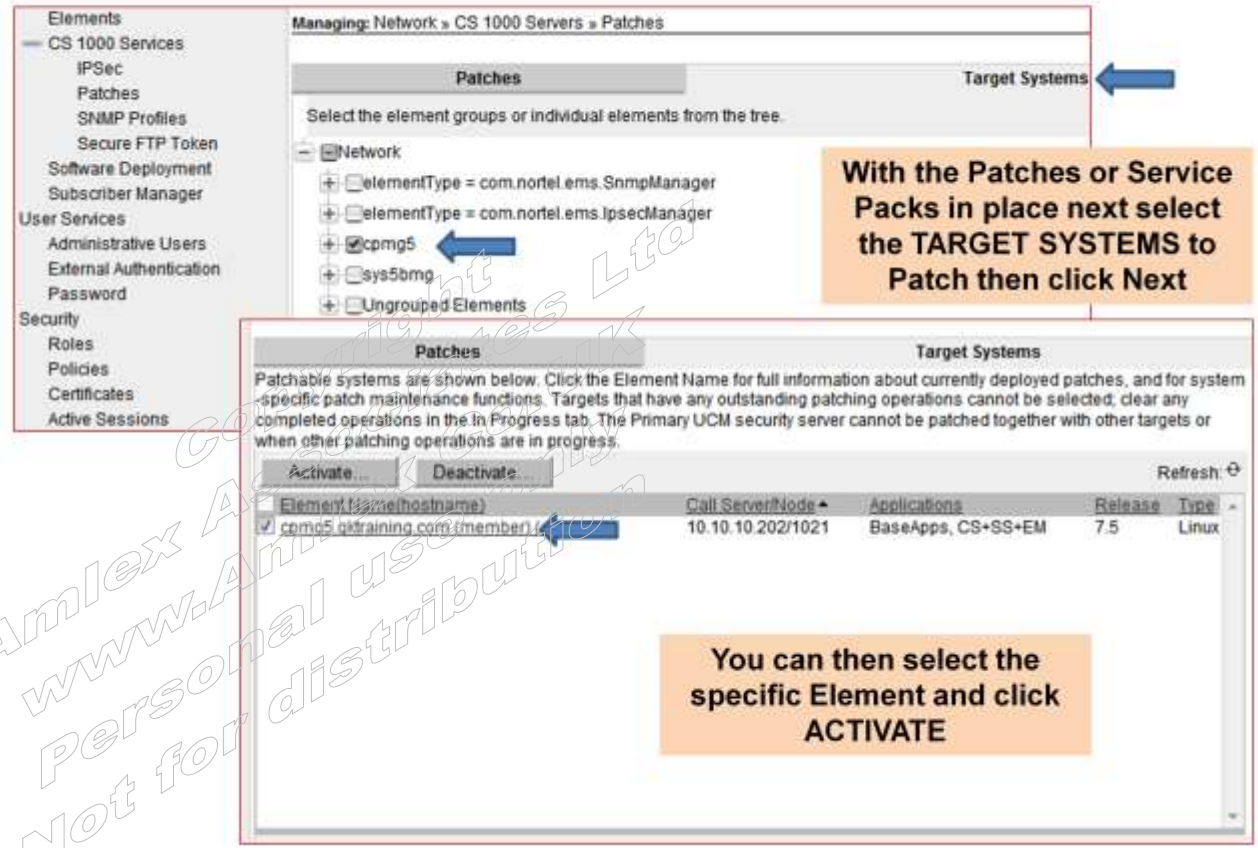
_____

Copyright Amlex Associates Ltd

Patch Process

To apply a patch you must first select the **TARGET SYSTEMS** tab and select a server using the tick box.

Once the server is allocated you are then prompted for which specific Element This is done by ticking the box and then clicking **ACTIVATE.**



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

200

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Patch Options

We are offered the Options for the Patch Type to be added and when we click NEXT we can select the patch to be applied.

At Rel 7 CoResident Call server patches and Loadware can be applied using the UCM Patch manager.

For the selected targets, choose the patch type for activation/de-activation
Patching updates
Patches(including binary patches)
Service pack, deplist
Note: For Co-resident elements only applies to Linux applications. Call Server has to be patched separately.
Co-resident Call Server
Patches
Deplists
Note: Co-resident Linux applications have to be patched separately
Loadware updates
IPMG loadware update
Distribute Patches
Step 1: Select a service pack,deplists or patches and loadware as per selected target.
Patches obtained from Avaya must be added to your patch library to be distributed to systems you have selected. Click the service pack or deplists or patches or loadware file name for more information.
Applicable patching
Patches
Refresh:
Patch Name
Date Created
Type
Release
Application
Special Instructions
Service impact
cs1000-tps-7.50.17.16-3.i386.000
Fri Apr 8 03:31:01 EDT 2011
RPM 7.50.17.00tps(SS)
NO
Restart tps
201

On this screen you will determine the type of Patch or Update being applied.

NOTE: Here you can see the option for CoRes call server as well as the Loadware updates

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Distribute Patches

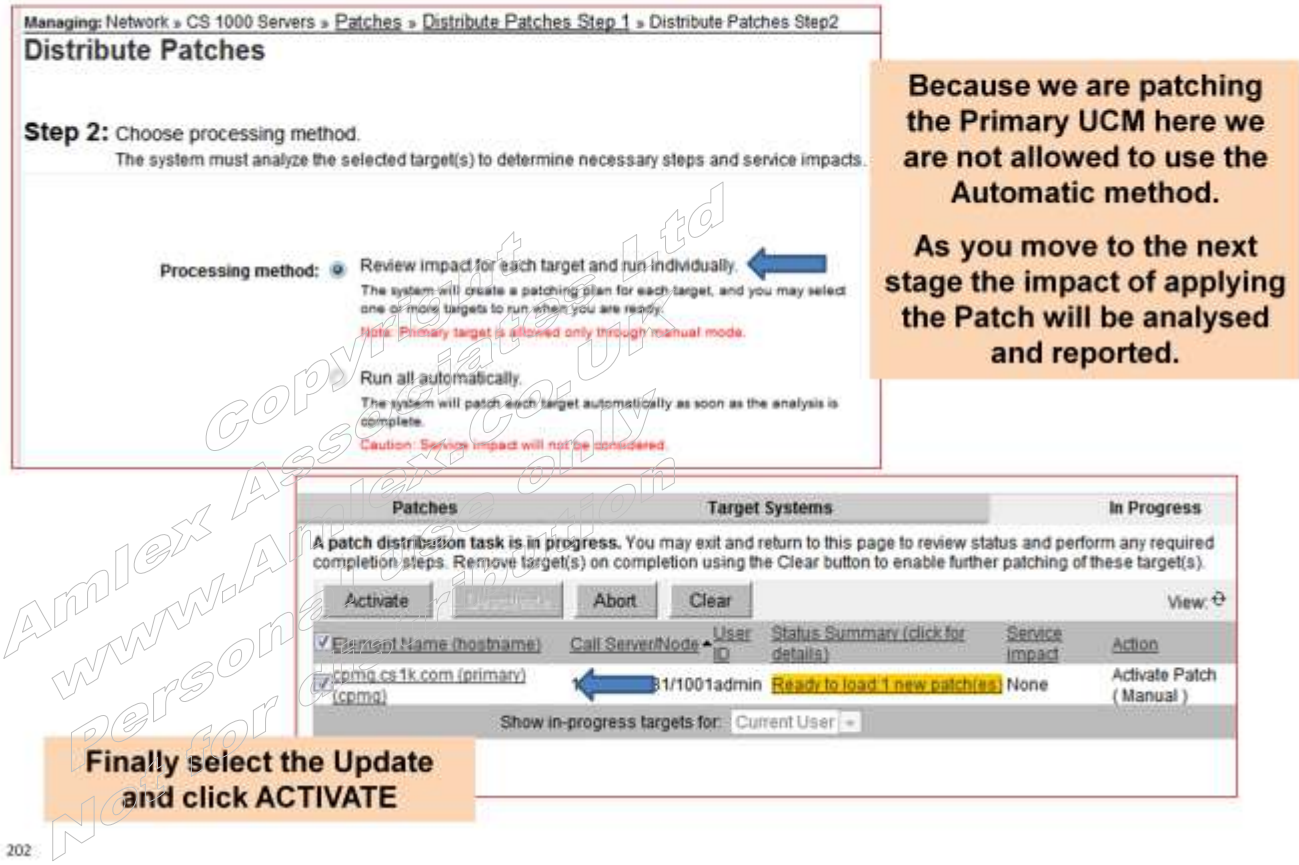
Here you can see the Status Summary (Yellow Highlight) outlining the service impact.

When you are ready to apply the patch select it again with the tick box and click the **ACTIVATE** button. Processing will start and you may well get the Completed message as shown at the bottom of the picture but remember in some cases the system may be going to reboot so you will need to wait for that to complete before logging back in.

Note:-
Once a centralised patching operation is completed you must clear it from the **IN PROGRESS** tab so that another operation can be selected. If you don't you will find you cannot select a server to apply a patch to.

Select the Completed message by the tick box and click he **CLEAR** button.

Note:-
To view the Patch status of a server you must go to the Base Manager of the particular server and use the Patch menu there.


Managing: Network » CS 1000 Servers » Patches » Distribute Patches Step 1 » Distribute Patches Step2
Distribute Patches
Step 2: Choose processing method.
The system must analyze the selected target(s) to determine necessary steps and service impacts.
Processing method:
Review impact for each target and run individually.
The system will create a patching plan for each target, and you may select one or more targets to run when you are ready.
Note: Primary target is allowed only through manual mode.
Run all automatically.
The system will patch each target automatically as soon as the analysis is complete.
Caution: Service impact will not be considered.
Because we are patching the Primary UCM here we are not allowed to use the Automatic method.
As you move to the next stage the impact of applying the Patch will be analysed and reported.
Patches
Target Systems
In Progress
A patch distribution task is in progress. You may exit and return to this page to review status and perform any required completion steps. Remove target(s) on completion using the Clear button to enable further patching of these target(s).
Activate
Abort
Clear
View:
Element Name (hostname)
Call Server/Node
User ID
Status Summary (click for details)
Service Impact
Action
cpmg.cs1k.com (primary) (cpmg)
1/1001admin
Ready to load 1 new patch(es)
None
Activate Patch (Manual)
Show in-progress targets for: Current User
Finally select the Update and click ACTIVATE

Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

202

Notes

_____

_____

_____

_____

Patching from Base Manager

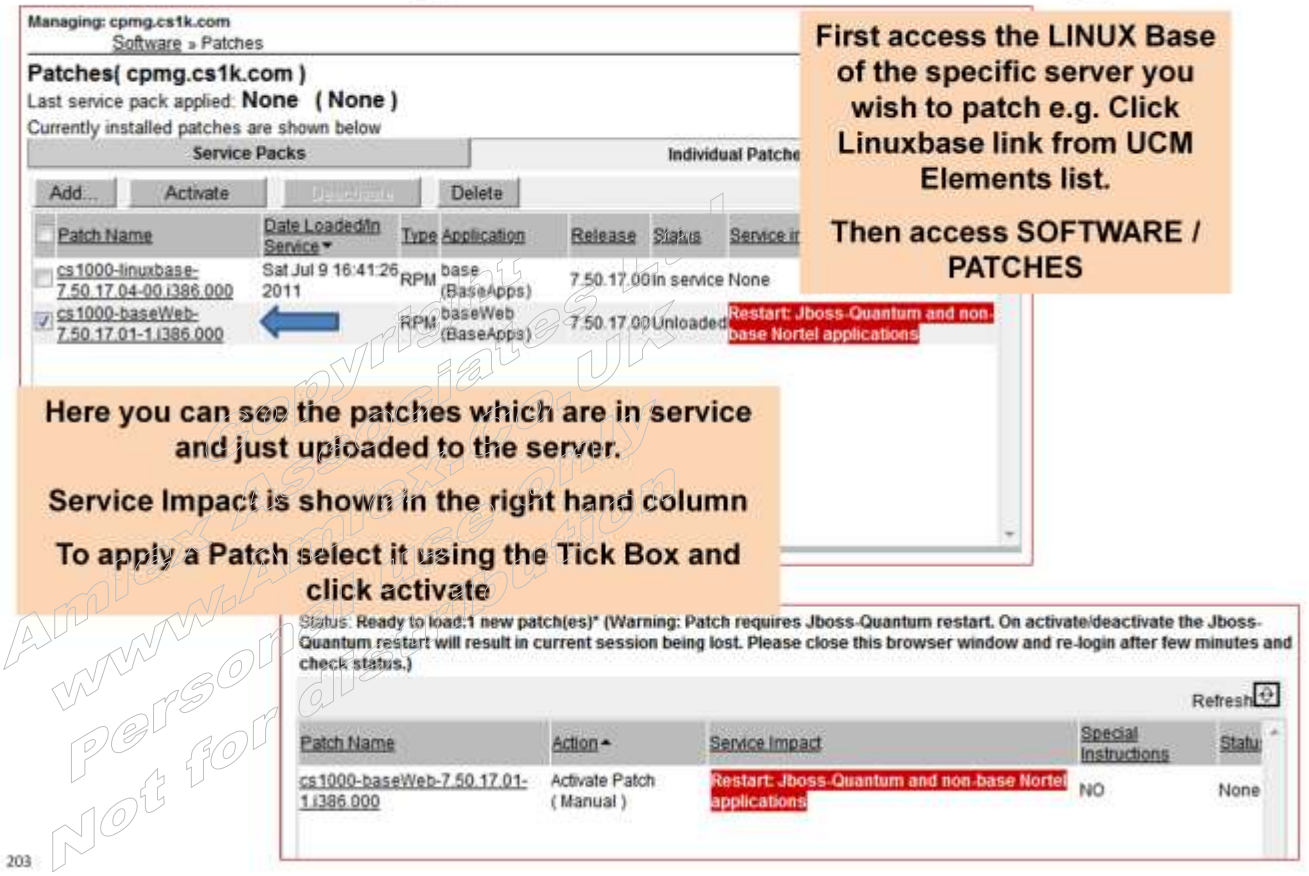
To patch a single server you must first enter the Base Manager for the server in question. (Use link in Elements list).

In the Base manager select the option **SOFTWARE / PATCHES**. You will then have the screens shown here and can upload the patches using the **ADD** button ready for activation. Alternatively you could use an SFTP client to copy the files to the relevant folder on the server :-
/var/opt/nortel/patch.

In the top screen shot you can see the patches that are currently In service and Unloaded.

To apply a patch use the tick box to select the patch to load and click the **ACTIVATE** button.

This will then display the second screen with the Service Impact outlined. If you are happy with the consequences click the **COMMIT** button to load the patch


Managing: cpmg.cs1k.com
Software » Patches
Patches(cpmg.cs1k.com)
Last service pack applied: None (None)
Currently installed patches are shown below
Service Packs
Individual Patche
Add...
Activate
Delete
Patch Name
Date Loaded/In Service
Type
Application
Release
Status
cs1000-linuxbase-7.50.17.04-00.i386.000
Sat Jul 9 16:41:26 2011
RPM
base (BaseApps)
7.50.17.00
in service
None
cs1000-baseWeb-7.50.17.01-1.i386.000
RPM
baseWeb (BaseApps)
7.50.17.00
Unloaded
Restart: Jboss-Quantum and non-base Nortel applications
First access the LINUX Base of the specific server you wish to patch e.g. Click Linuxbase link from UCM Elements list.
Then access SOFTWARE / PATCHES
Here you can see the patches which are in service and just uploaded to the server.
Service Impact is shown in the right hand column
To apply a Patch select it using the Tick Box and click activate
Status: Ready to load:1 new patch(es)* (Warning: Patch requires Jboss-Quantum restart. On activate/deactivate the Jboss-Quantum restart will result in current session being lost. Please close this browser window and re-login after few minutes and check status.)
Refresh
Patch Name
Action
Service Impact
Special Instructions
Statu
cs1000-baseWeb-7.50.17.01-1.i386.000
Activate Patch (Manual)
Restart: Jboss-Quantum and non-base Nortel applications
NO
None
203

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Patching through Linux CLI

To apply patches via the Linux command line you need first to copy them to the correct location.

Patch files need to be located in **/var/opt/nortel/patch**

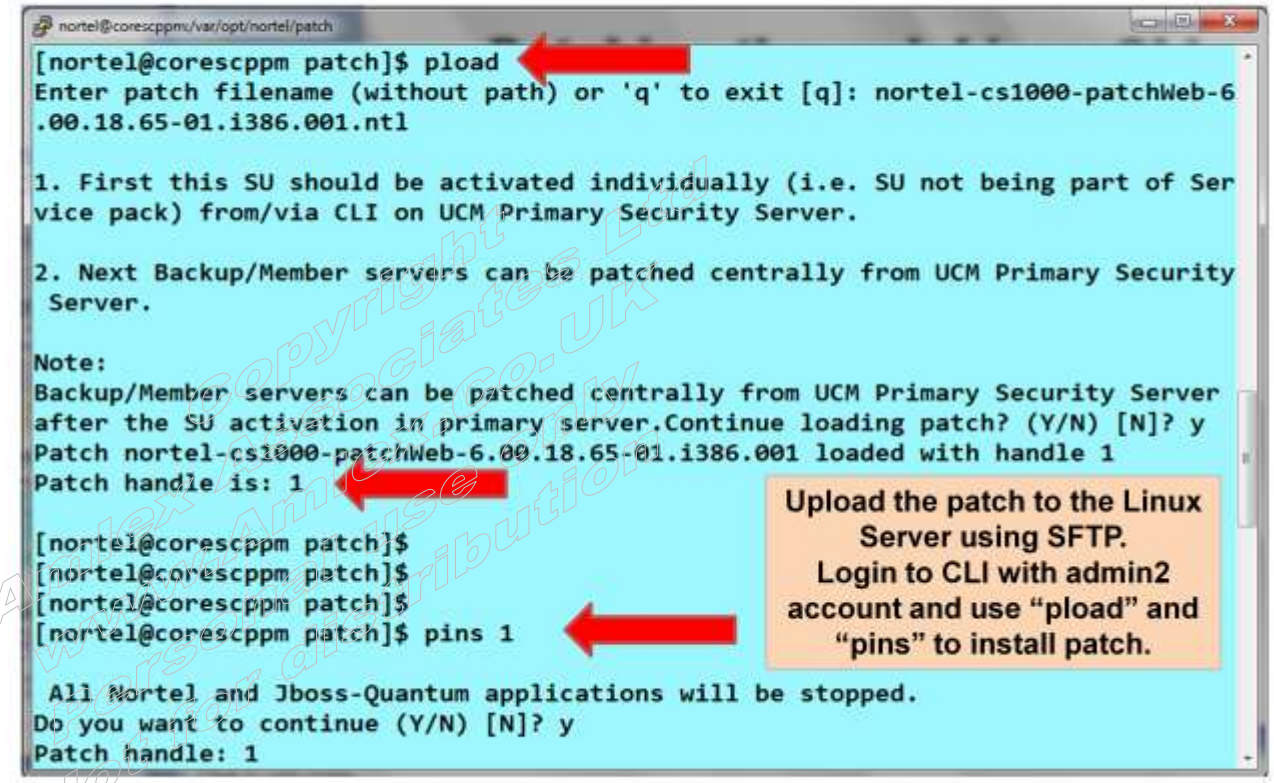
Service Packs need to be located in **/var/opt/nortel/patch/sp**

Once the files are in place on the server login with the admin2 account and issue the command:-
pload

-this loads the patch and adds a handle and will ask for the patch filename.

The system will respond an return the Patch Handle allocated.

Next issue the command :-
pins <handle no.> - this brings the patch into service. It will warn you of any service impact at this point and offer you the choice to quit.


nortel@corescppm:/var/opt/nortel/patch
[nortel@corescppm patch]$ pload
Enter patch filename (without path) or 'q' to exit [q]: nortel-cs1000-patchWeb-6
.00.18.65-01.i386.001.ntl
1. First this SU should be activated individually (i.e. SU not being part of Ser
vice pack) from/via CLI on UCM Primary Security Server.
2. Next Backup/Member servers can be patched centrally from UCM Primary Security
Server.
Note:
Backup/Member servers can be patched centrally from UCM Primary Security Server
after the SU activation in primary server.Continue loading patch? (Y/N) [N]? y
Patch nortel-cs1000-patchWeb-6.00.18.65-01.i386.001 loaded with handle 1
Patch handle is: 1
[nortel@corescppm patch]$
[nortel@corescppm patch]$
[nortel@corescppm patch]$
[nortel@corescppm patch]$ pins 1
All Nortel and Jboss-Quantum applications will be stopped.
Do you want to continue (Y/N) [N]? y
Patch handle: 1
Upload the patch to the Linux Server using SFTP.
Login to CLI with admin2 account and use "pload" and "pins" to install patch.

204

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Patch Status Linux CLI

Here you can see the tail end of the patch load sequence followed by the message that the UCM is now back in service.

To view the patch status of the server issue the command :-
pstat - This will show the currently loaded patches for the system.

To take a patch out of service use the command :-
pout

Note:-

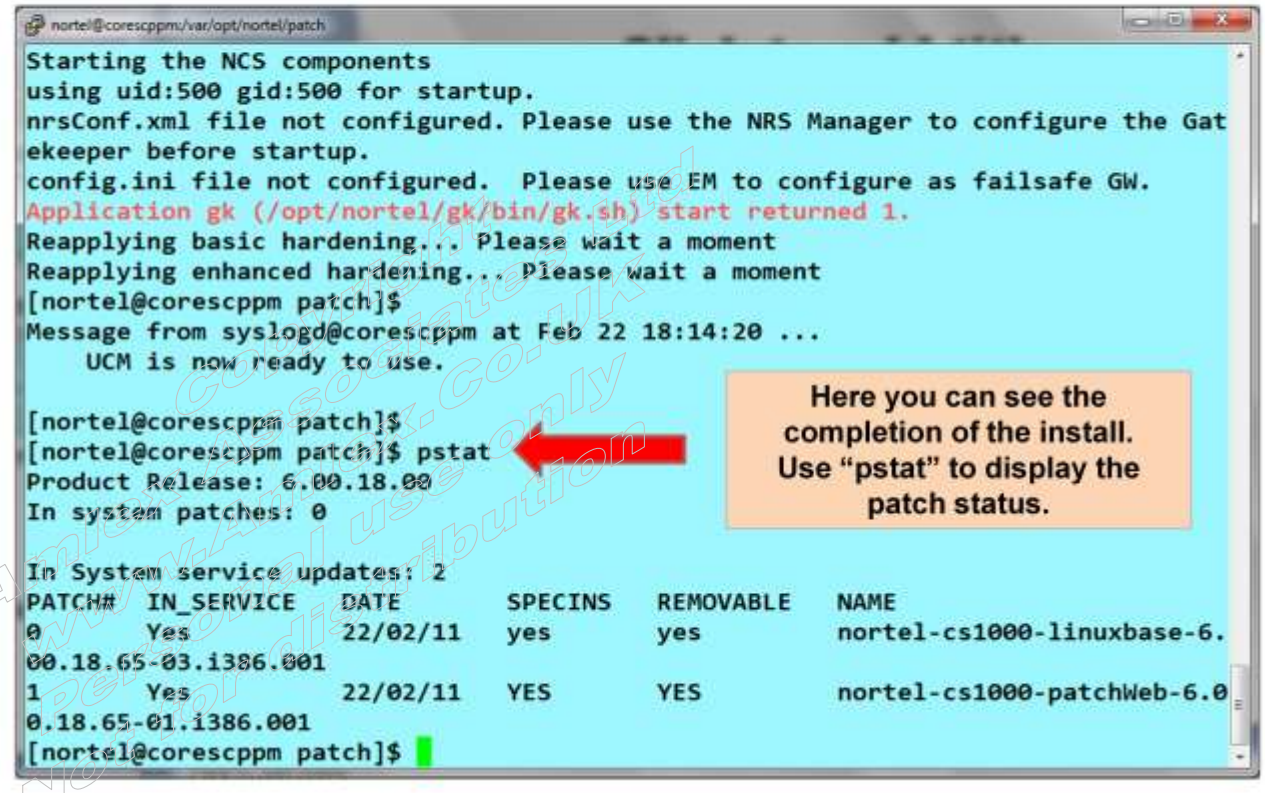
To load and apply a service pack the sequence is the same but the relevant commands are :-

sload

spins

spstat

spout


nortel@corescppm:/var/opt/nortel/patch
Starting the NCS components
using uid:500 gid:500 for startup.
nrsConf.xml file not configured. Please use the NRS Manager to configure the Gatekeeper before startup.
config.ini file not configured. Please use EM to configure as failsafe GW.
Application gk (/opt/nortel/gk/bin/gk.sh) start returned 1.
Reapplying basic hardening... Please wait a moment
Reapplying enhanced hardening... Please wait a moment
[nortel@corescppm patch]$
Message from syslogd@corescppm at Feb 22 18:14:20 ...
UCM is now ready to use.
[nortel@corescppm patch]$
[nortel@corescppm patch]$ pstat
Product Release: 6.00.18.00
In system patches: 0
In System service updates: 2
PATCH# IN_SERVICE DATE SPECINS REMOVABLE NAME
0 Yes 22/02/11 yes yes nortel-cs1000-linuxbase-6.00.18.65-03.i386.001
1 Yes 22/02/11 YES YES nortel-cs1000-patchWeb-6.00.18.65-01.i386.001
[nortel@corescppm patch]$
Here you can see the completion of the install. Use "pstat" to display the patch status.

205

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Call Server Patching

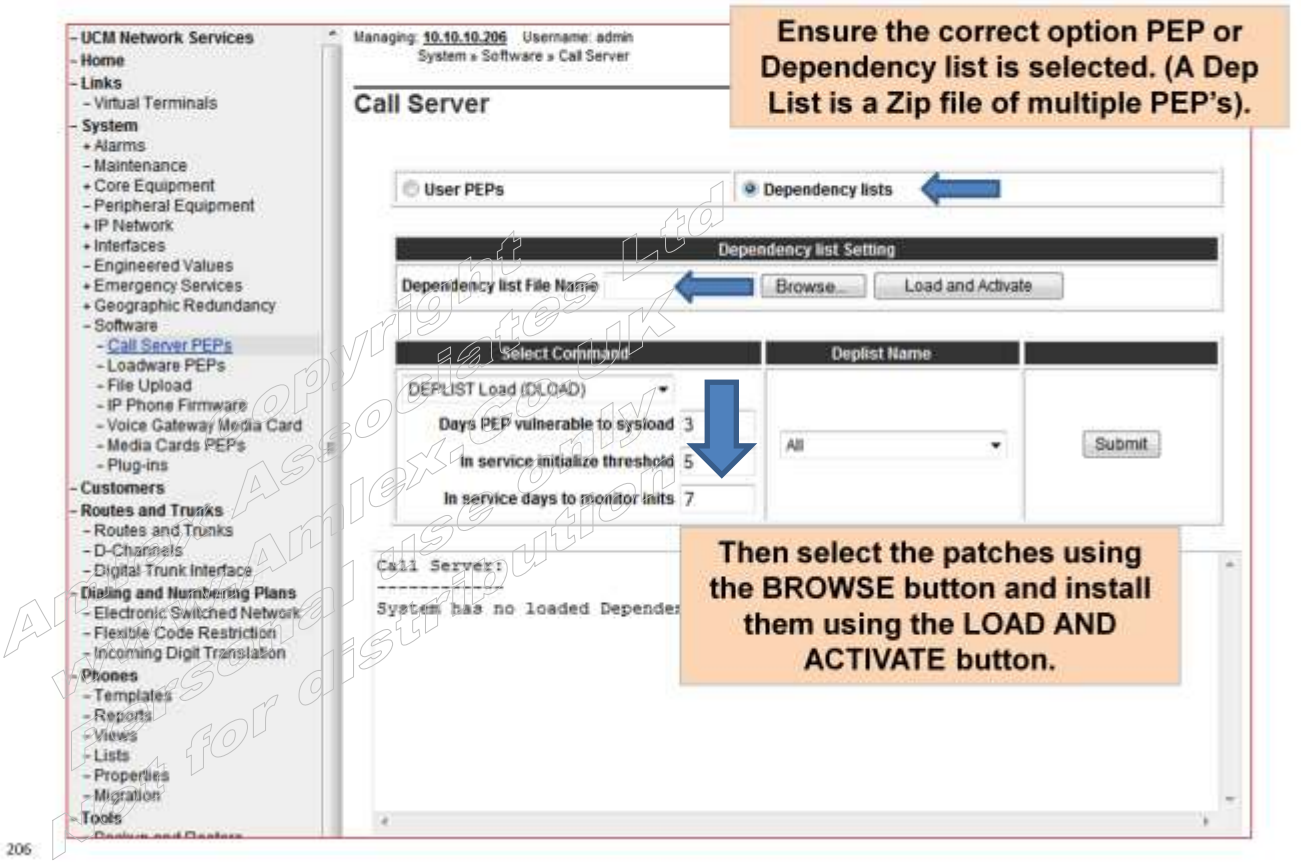
The Call Server can also be patched through the Element Manager as shown here.

Access this screen from **SYSTEM / SOFTWARE / CALL SERVER PEPS** .

To add a PEP or DEPLIST select the appropriate tab and then **BROWSE** to the PEP or DEPLIST.

Select the appropriate settings for vulnerability to sysload, initialise threshold and in service days (Arrowed). These are used to control how the patch will react in case there is an issue

Once these settings are completed click the **LOAD AND ACTIVATE** button to bring the patches into service.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

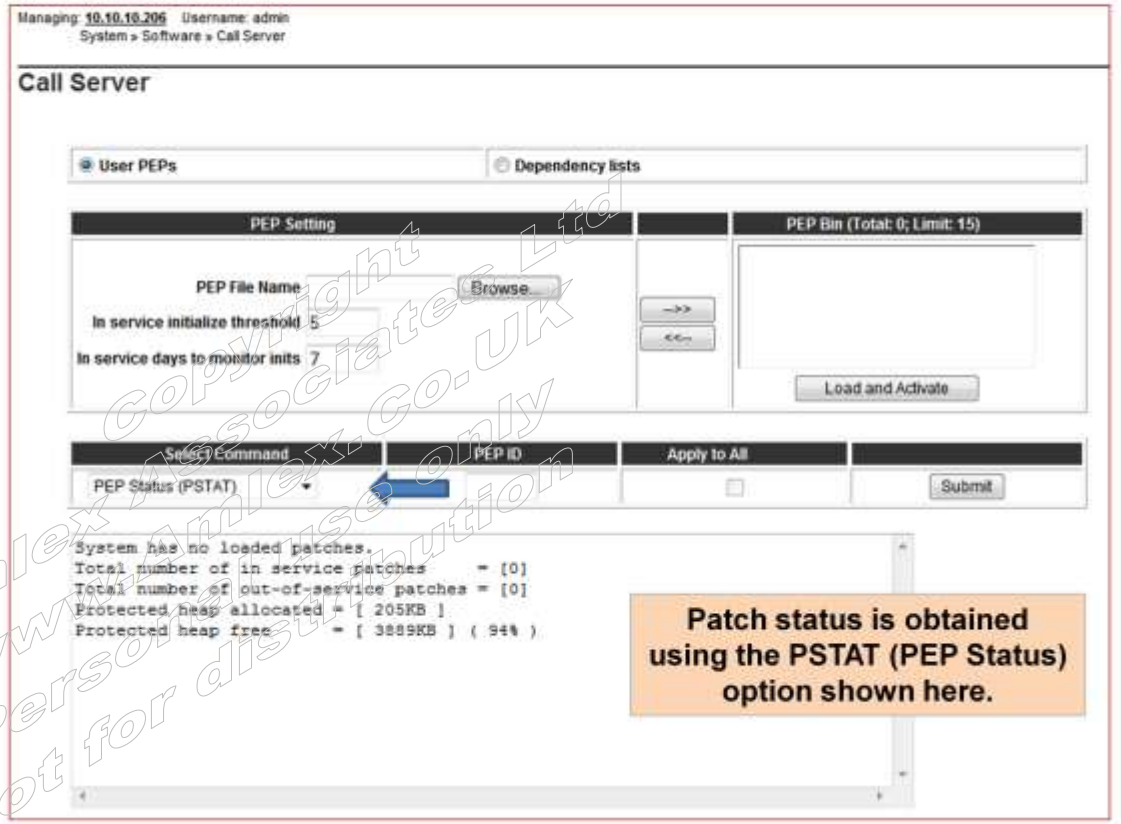
Review in Service PEP's

To review the patches installed on the call server select the **USER PEP** tab.

Ensure the Select Command setting is set to **PEP STATUS (PSTAT)** and click the **SUBMIT** button.

The resuls will be displayed in the lower window for you to review. The example shows patch p28657 from a core dependency list.

Deplists and PEP's can also be loaded from PDT.


Managing: 10.10.10.206 Username: admin
System » Software » Call Server
Call Server
User PEPs
Dependency lists
PEP Setting
PEP Bin (Total: 0; Limit: 15)
PEP File Name
Browse...
In service initialize threshold 5
In service days to monitor inits 7
Load and Activate
Select Command
PEP ID
Apply to All
PEP Status (PSTAT)
Submit
System has no loaded patches.
Total number of in service patches = [0]
Total number of out-of-service patches = [0]
Protected heap allocated = [205KB]
Protected heap free = [3889KB] (94%)
Patch status is obtained using the PSTAT (PEP Status) option shown here.
207

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

20. CoRes Call server

• Install Linux Base		
– Same as for HA or SA	Section 1-6	Page 67
• Run Security Configuration		
– Select Server Role	Section 1-7	Page 85
• Primary/Backup/Member		
• Login to UCM		
– Check Linux Base element has registered		
• Deploy Software Applications		
– Add software load	Section 1-8	Page 106
– Deploy CoRes Call Server	Section 2-20	Page 204
• Access Call server from Linux CLI		
– csconsole / cslogin	Section 2-20	Page 216
– Initial Call Server Config	Section 1-5	Page 56
• Complete Configuration		
– Add Media Gateway	Section 1-9	Page 113
– Join UCM	Section 2-10	Page 130
– IP Telephony Node	Section 2-11	Page 133

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

208

Notes

_____

_____

_____

_____

Application Selection

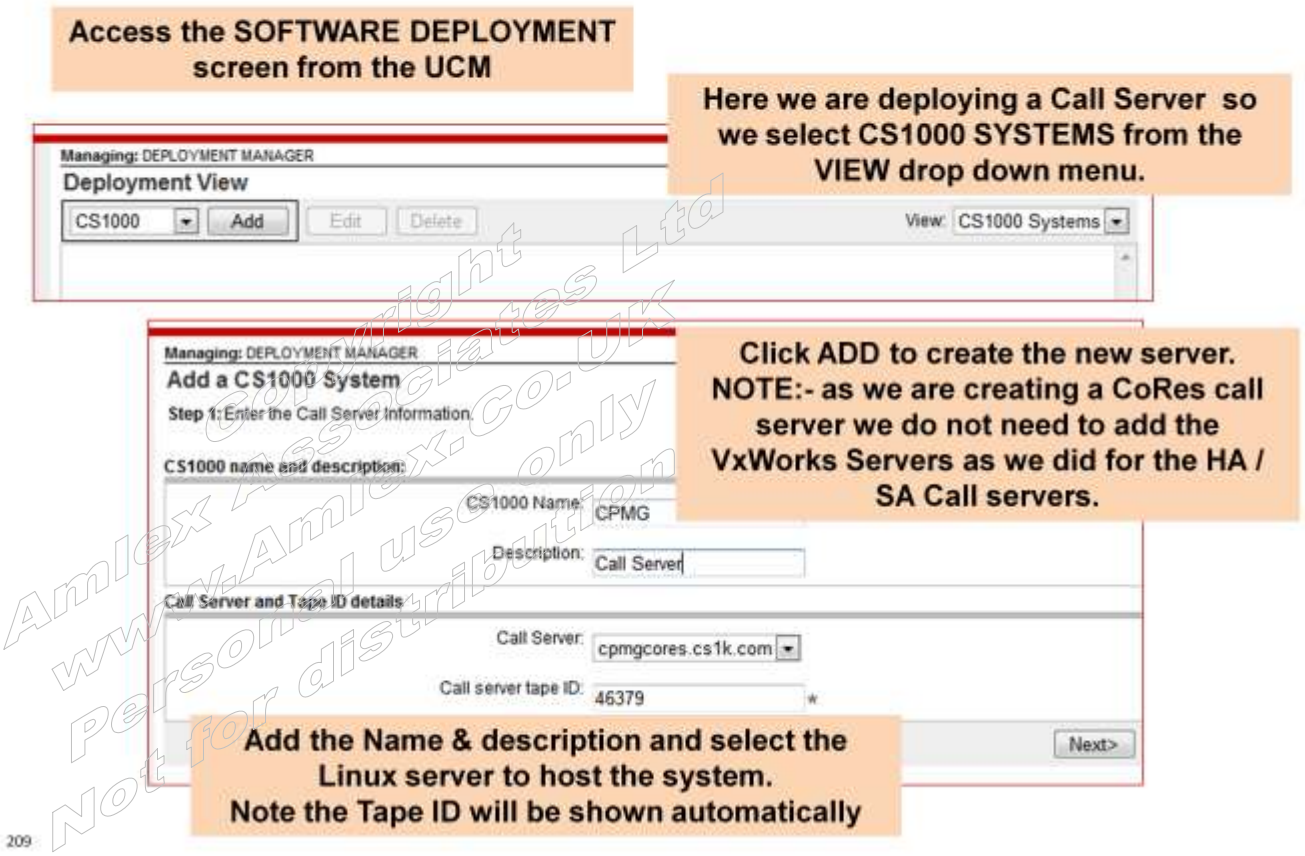
Having selected CS1000 Systems from the VIEW menu the left hand dialogue box will change from Linux to CS1000 or CS1000 HS (High Scalability).

As we are configuring a CoResident call server we will leave the selection as CS1000 and click the ADD button.

This will then open the lower scren prompting for a Name and description.

It will also select the FQDN of the Linux server and Tape ID.

Clicking NEXT will take us onto the next stage.


Access the SOFTWARE DEPLOYMENT screen from the UCM
Here we are deploying a Call Server so we select CS1000 SYSTEMS from the VIEW drop down menu.
Managing: DEPLOYMENT MANAGER
Deployment View
CS1000
Add
Edit
Delete
View: CS1000 Systems
Managing: DEPLOYMENT MANAGER
Add a CS1000 System
Step 1: Enter the Call Server information.
CS1000 name and description:
CS1000 Name: CPMG
Description: Call Server
Call Server and Tape ID details
Call Server: cpmgcores.cs1k.com
Call server tape ID: 46379
Next>
Click ADD to create the new server.
NOTE:- as we are creating a CoRes call server we do not need to add the VxWorks Servers as we did for the HA / SA Call servers.
Add the Name & description and select the Linux server to host the system.
Note the Tape ID will be shown automatically
209

Copyright Amlex Associates Ltd
www.Amlex-Co.Uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Select & Validate Keycode

As we are deploying a Call Server in this example the system will prompt us for a Keycode to match the installed Dongle and activate the different options for the system.

Select the keycode either from the device in the RMD slot or from the client PC you are working from.

When you click the **VALIDATE** button the system will check the Keycode match to the installed security “Dongle” as the Linux systems is already deployed.. In this way we know that the keycode is correct before the system is actually installed.

Managing: DEPLOYMENT MANAGER
Add a CS1000 call server
Step 2: Pre-configuration for the linux call server. Keycode uploading and validation. Language and databa
Host name: cpmgcores
Select the Keycode file to upload and click Validate button to validate and upload the file.
Select keycode location: Deployment Server
Media: USB Device
Browse
Keycode file: keycode/4121_CPPM_Co-res_7.0.kcd
Validate

Because we are deploying a Call Server we are prompted for a valid Keycode file.
Select the location and file and click VALIDATE to ensure it is correct.

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

210

Notes

_____

_____

_____

_____

Select Customer Database

Now we are prompted for the Language files we wish to use and the database to upload to the system. The Language files are those which can be selected for prompts etc.

In the Labs we will likely use the Default Database but in an upgrade scenario we would use the customers database. The Default database is an empty system with very little configured. If you have pre-configured systems as starting points these may well be used at this stage.

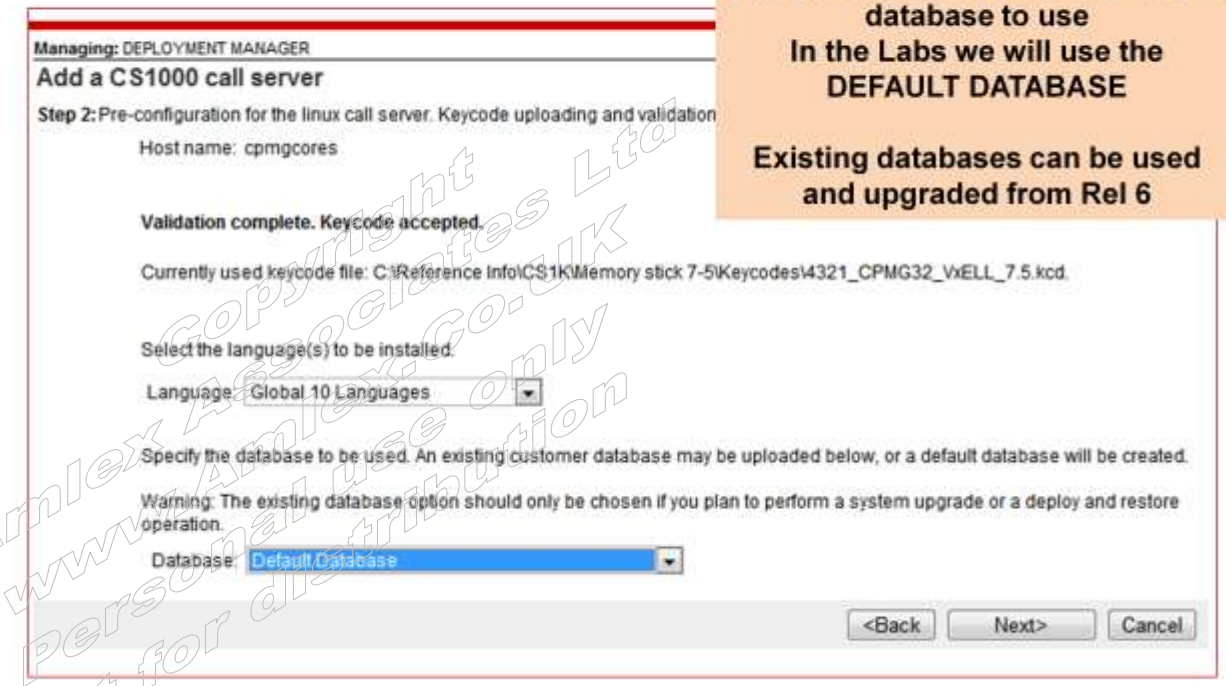
The database can be located on the RMD or client PC. However if the Database has been copied from one medium to another be sure to maintain the directory structure it was created in e.g.

arch_db/sys2

for an archived database from a “Small System” as the system uses this to recognise how to convert the data.

Again because we are deploying a Call Server we will be asked for the database to use
In the Labs we will use the DEFAULT DATABASE

Existing databases can be used and upgraded from Rel 6


Managing: DEPLOYMENT MANAGER
Add a CS1000 call server
Step 2: Pre-configuration for the linux call server. Keycode uploading and validation
Host name: cpmgcores
Validation complete. Keycode accepted.
Currently used keycode file: C:\Reference Info\CS1K\Memory stick 7-5\Keycodes\4321_CPMG32_VxELL_7.5.kcd
Select the language(s) to be installed.
Language: Global 10 Languages
Specify the database to be used. An existing customer database may be uploaded below, or a default database will be created.
Warning: The existing database option should only be chosen if you plan to perform a system upgrade or a deploy and restore operation.
Database: Default Database
<Back
Next>
Cancel

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

211

Notes

_____

_____

_____

_____

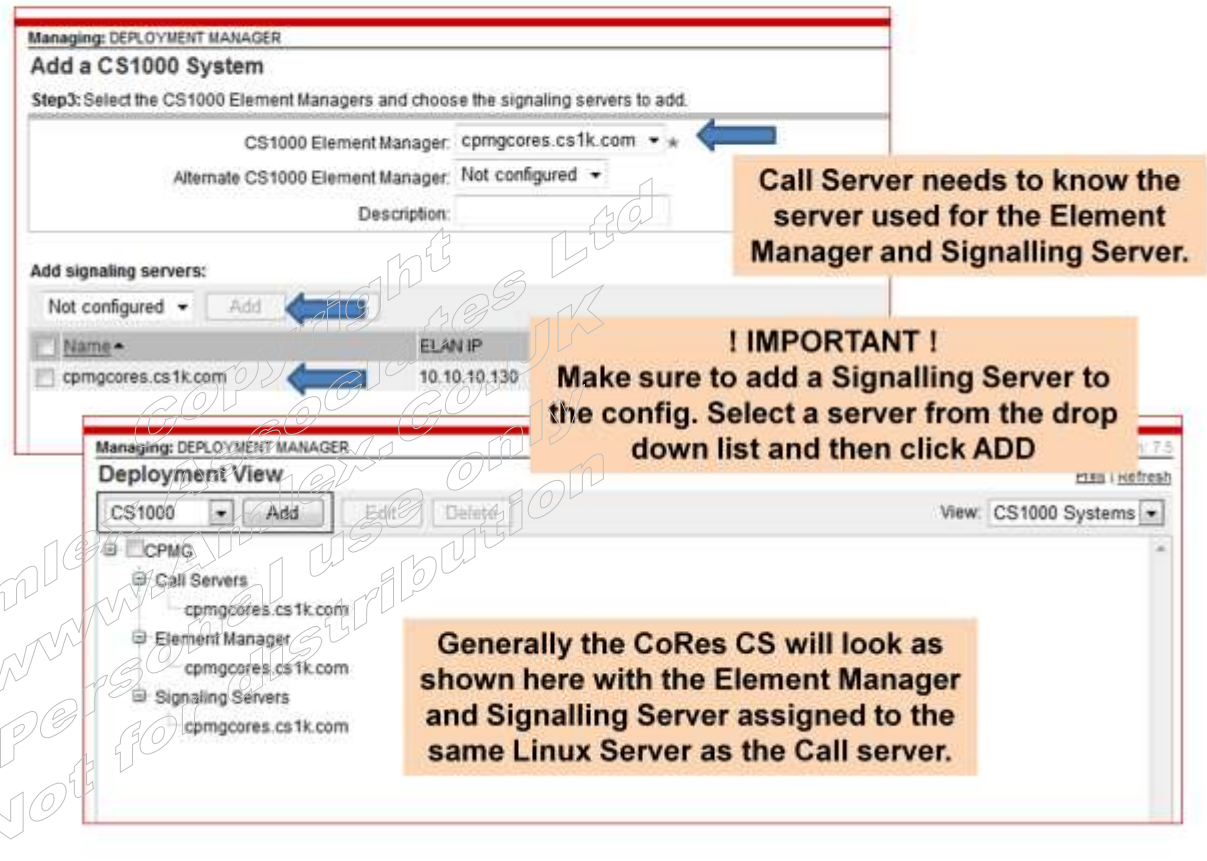
As we are deploying an Element manager it is necessary to define which call server it is managing.

As the example is for a CoRes call server and we only have one deployed server currently, it automatically assumes the Element Manager will be deployed on that server. As you can see it also prompts for an Alternate Element Manager if one is available.

In addition we need to define the signalling servers that the system will use. Again as we are creating a CoRes server the Signalling server will be the same as the Element Manager and Call Server. This can be seen in the Lower screen shot.

The configuration is now completed we finish it off using the button at the bottom of the screen.

Target for Element Manager


Managing: DEPLOYMENT MANAGER
Add a CS1000 System
Step3: Select the CS1000 Element Managers and choose the signaling servers to add.
CS1000 Element Manager: cpmgcores.cs1k.com
Alternate CS1000 Element Manager: Not configured
Description:
Add signaling servers:
Not configured
Add
Name
ELAN IP
cpmgcores.cs1k.com
10.10.10.130
Call Server needs to know the server used for the Element Manager and Signalling Server.
! IMPORTANT !
Make sure to add a Signalling Server to the config. Select a server from the drop down list and then click ADD
Managing: DEPLOYMENT MANAGER
Deployment View
CS1000
Add
Edit
Delete
View: CS1000 Systems
CPMG
Call Servers
cpmgcores.cs1k.com
Element Manager
cpmgcores.cs1k.com
Signaling Servers
cpmgcores.cs1k.com
Generally the CoRes CS will look as shown here with the Element Manager and Signalling Server assigned to the same Linux Server as the Call server.

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

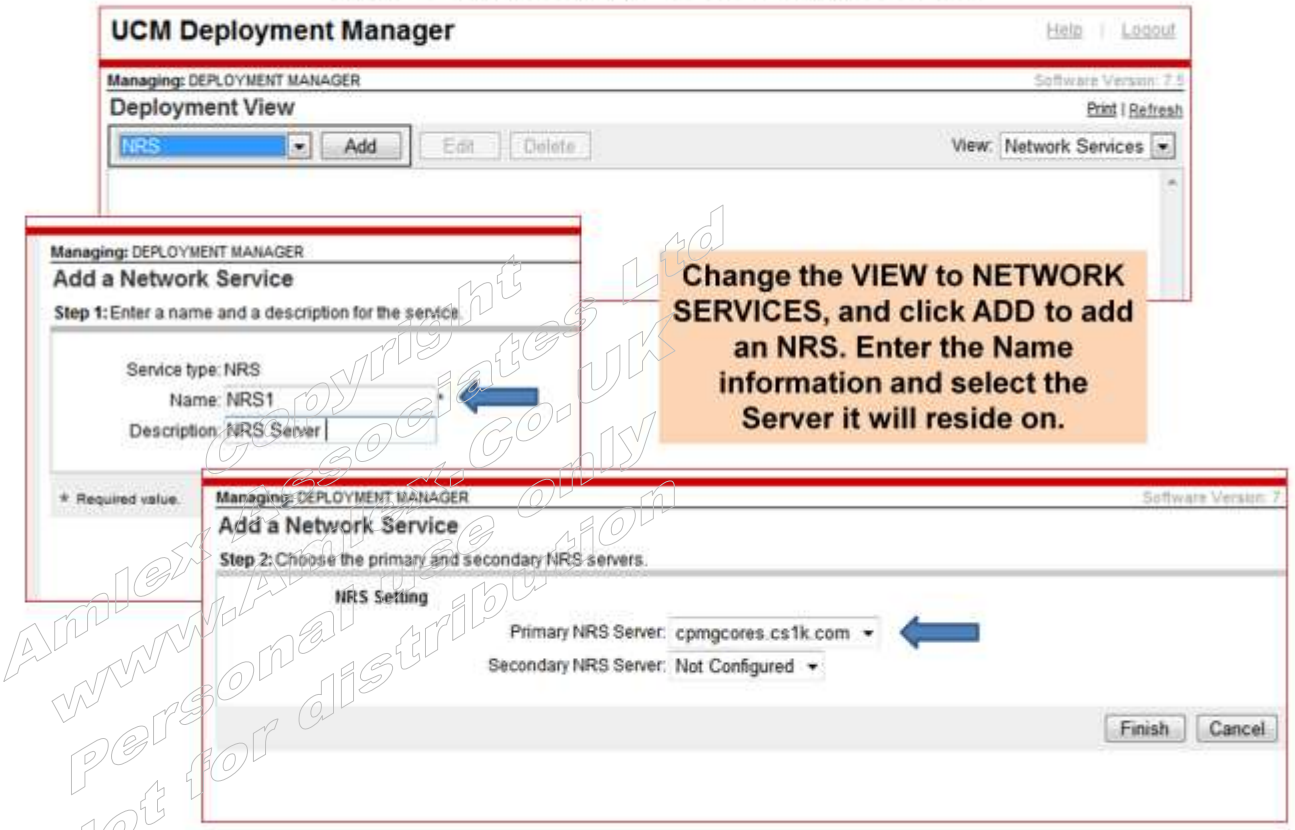
_____

Copyright Amlex Associates Ltd

Network Services

If we want to add further services to the server we can swap to the NETWORK SERVICES view and again the left hand dialogue will change offering us to add an NRS or Subscriber Manager.

We will add both the NRS and the Subscriber manager to our servers


UCM Deployment Manager
Help | Logout
Managing: DEPLOYMENT MANAGER
Deployment View
Print | Refresh
NRS
Add
Edit
Delete
View: Network Services
Managing: DEPLOYMENT MANAGER
Add a Network Service
Step 1: Enter a name and a description for the service.
Service type: NRS
Name: NRS1
Description: NRS Server
* Required value.
Change the VIEW to NETWORK SERVICES, and click ADD to add an NRS. Enter the Name information and select the Server it will reside on.
Managing: DEPLOYMENT MANAGER
Add a Network Service
Step 2: Choose the primary and secondary NRS servers.
NRS Setting
Primary NRS Server: cpmgcores.cs1k.com
Secondary NRS Server: Not Configured
Finish
Cancel

213

Notes

_____

_____

_____

_____

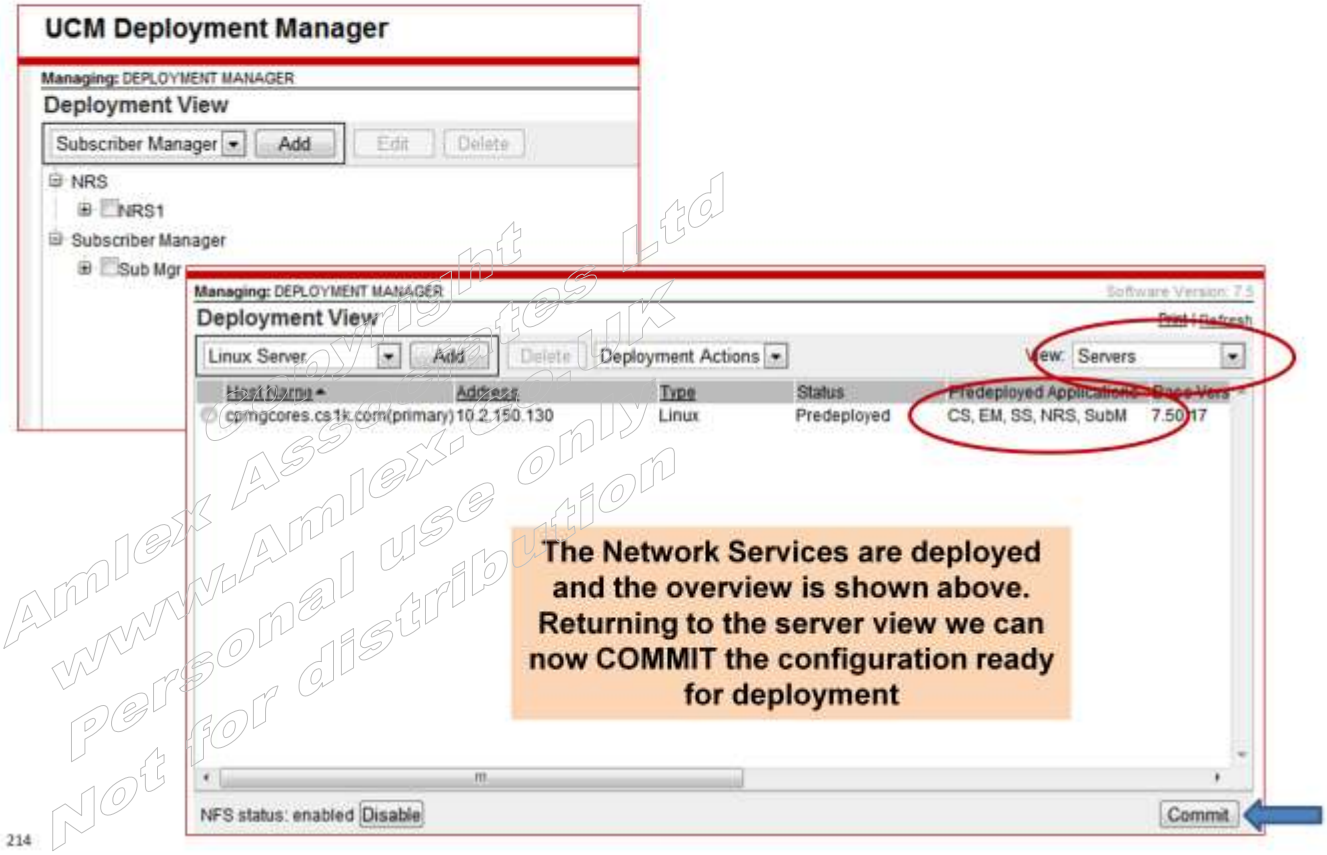
Copyright Amlex Associates Ltd

Completed Config - Commit

In these two screens we can see the completed NRS and Subscriber Manager and then by switching to the SERVERS view in the Right Hand menu again we will se the original Linux server now has a full list of Pre-Deployed applications

- CS, EM, SS, NRS, SubM

The next step is to COMMIT the configuration, this stops further changes and it is then in a state ready to DEPLOY to the actual server.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

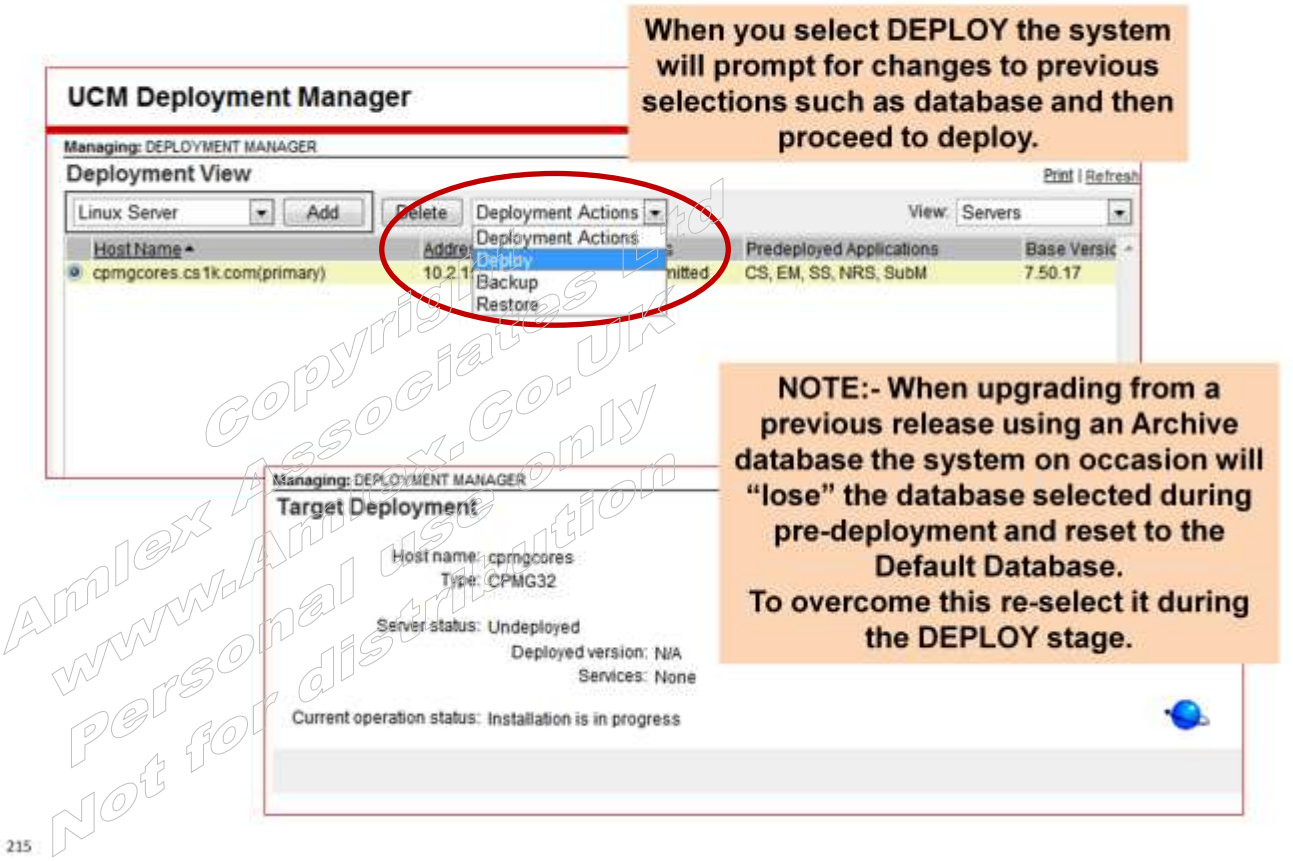
_____

Deployment

Once the pre-deployment is complete and committed you will be able to select the DEPLOY option from the Centre dropdown menu as shown.

The system will then start to copy and install the requested applications. In this instance it is actually deploying to itself but of course this could be another server located anywhere on the network.

When the installation is completed the display will report this and you can then navigate back to the main ELEMENTS list to access the applications installed.



Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

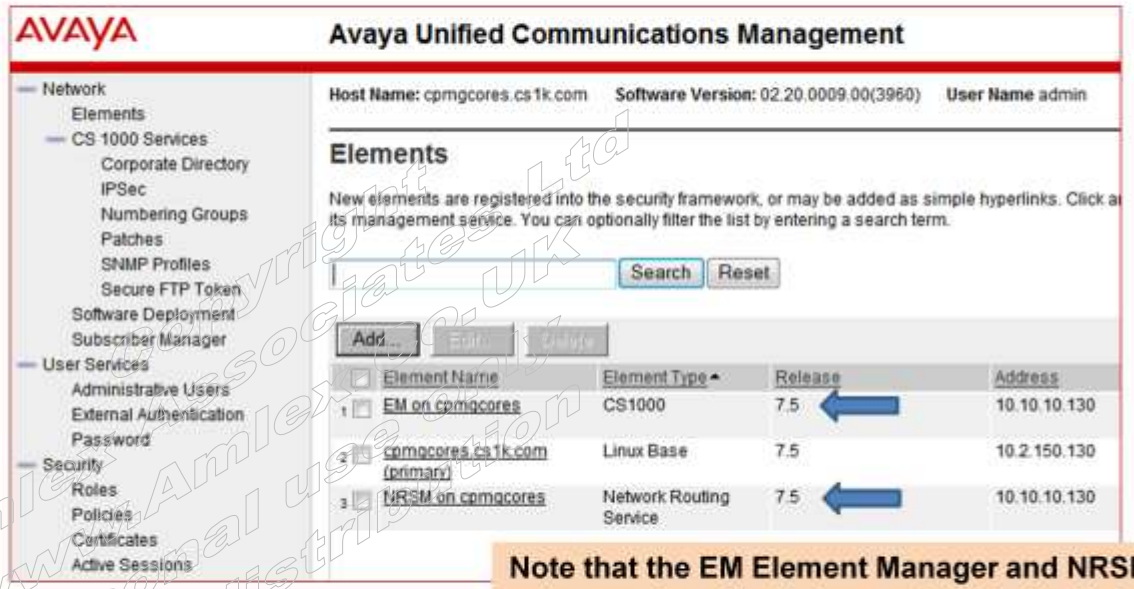
_____

Copyright Amlex Associates Ltd

Element List after Deployment

Returning to the UCM Elements list will now display two additional entries for the Element Manager on the call server and the NRSM. Originally you would only have had the Linux Base entry in the list i.e. The Linux server itself.

If you need to edit any of the details, the description for instance, select the entry using the tick box as shown, then click on the **EDIT** button.



Note that the EM Element Manager and NRSM have automatically been added to the list

Use the EDIT button to change any details such as the name or description

Amlex Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

216

Notes

_____

_____

_____

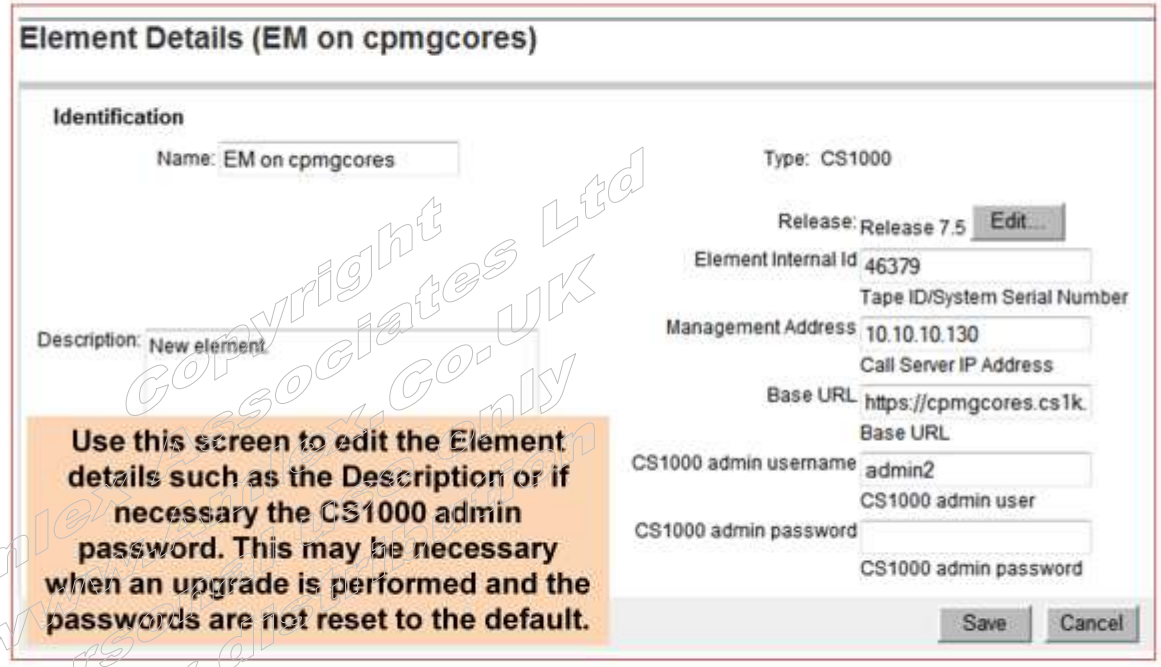
_____

Copyright Amlex Associates Ltd

Editing Element Details

Here is the edit screen where you can change the description field to make it more relevant to the system.

In some circumstances, such as upgrading a customer system you may need to edit the “admin2” password field to match the database installed as the UCM assumes the default password (0000) when it creates the entry.


Element Details (EM on cpmgcores)
Identification
Name: EM on cpmgcores
Type: CS1000
Release: Release 7.5
Edit...
Element Internal Id 46379
Tape ID/System Serial Number
Management Address 10.10.10.130
Call Server IP Address
Base URL https://cpmgcores.cs1k.
Base URL
CS1000 admin username admin2
CS1000 admin user
CS1000 admin password
CS1000 admin password
Description: New element
Use this screen to edit the Element details such as the Description or if necessary the CS1000 admin password. This may be necessary when an upgrade is performed and the passwords are not reset to the default.
Save
Cancel

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

217

Notes

_____

_____

_____

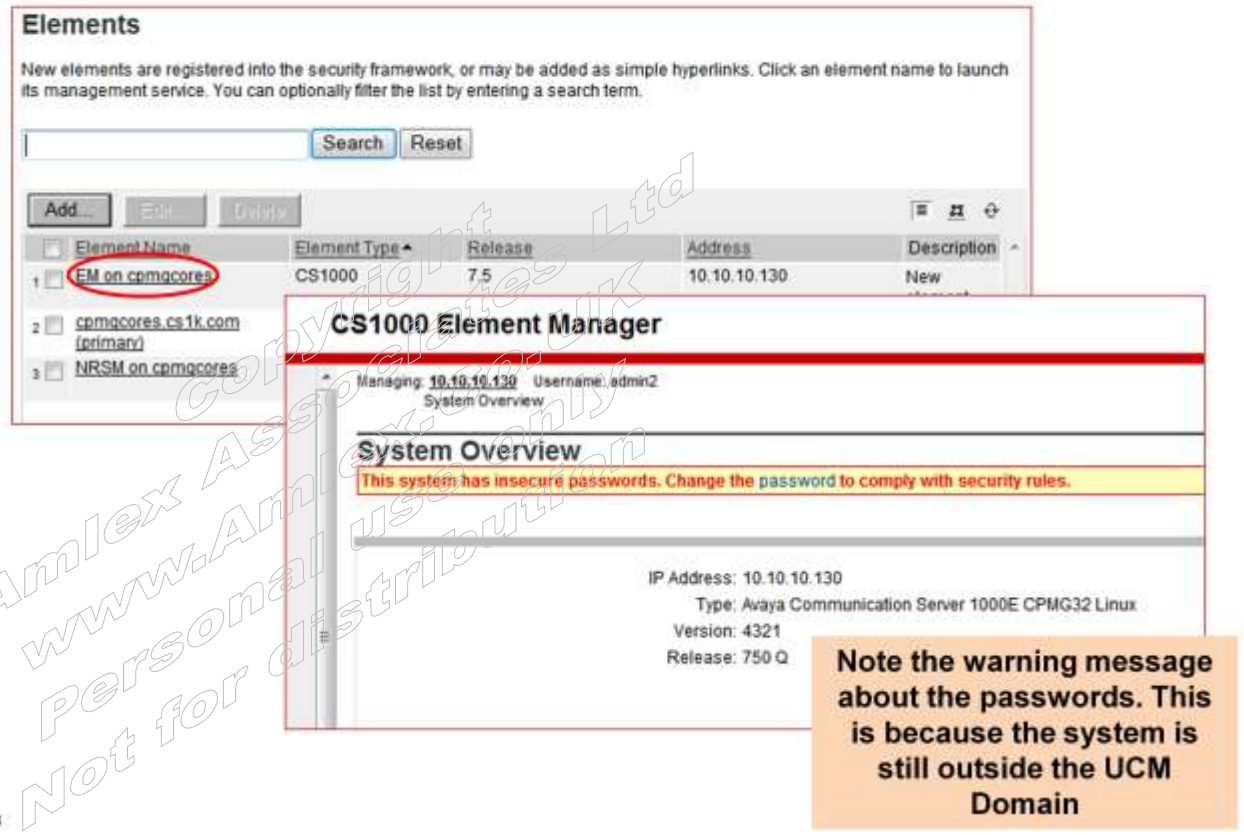
_____

Access Element Manager

To access the Element Manager for the CoRes system just click on the circled link in the diagram. This will navigate you to the Element manager for the system as shown in the lower screen shot without having to login again. This is the Single Sign On concept in action.

Note the Yellow banner message on the lower screen warning of an insecure password. This is because the call server has not yet been brought into the UCM domain and is still using the "admin2" login with default password.

Once the system is fully registered to the UCM domain this will no longer be shown.



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

Notes

_____

_____

_____

_____

CoRes Call Server CLI

To access the Call Server you can use either the Console com port and a Serial connection or access via the network using a terminal emulator that supports SSH.

As you can se here we are using PuTTY which is ideal for connecting across the network.

Note that SSH is secure in its connection hence its preference to Telnet which is disabled by default on the Linux Base.

If you are accessing a Standard Availability or High Availability system (VxWorks based) SSH can still be used but you will need to configure the IP addressing for the Call Server first using the Console port.

- Access Via the Console Com Port
  - 9600 8 none 1 stop
- Access via SSH across network
  - Use PuTTY or similar to connect

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution © Copyright

219

Notes

_____

_____

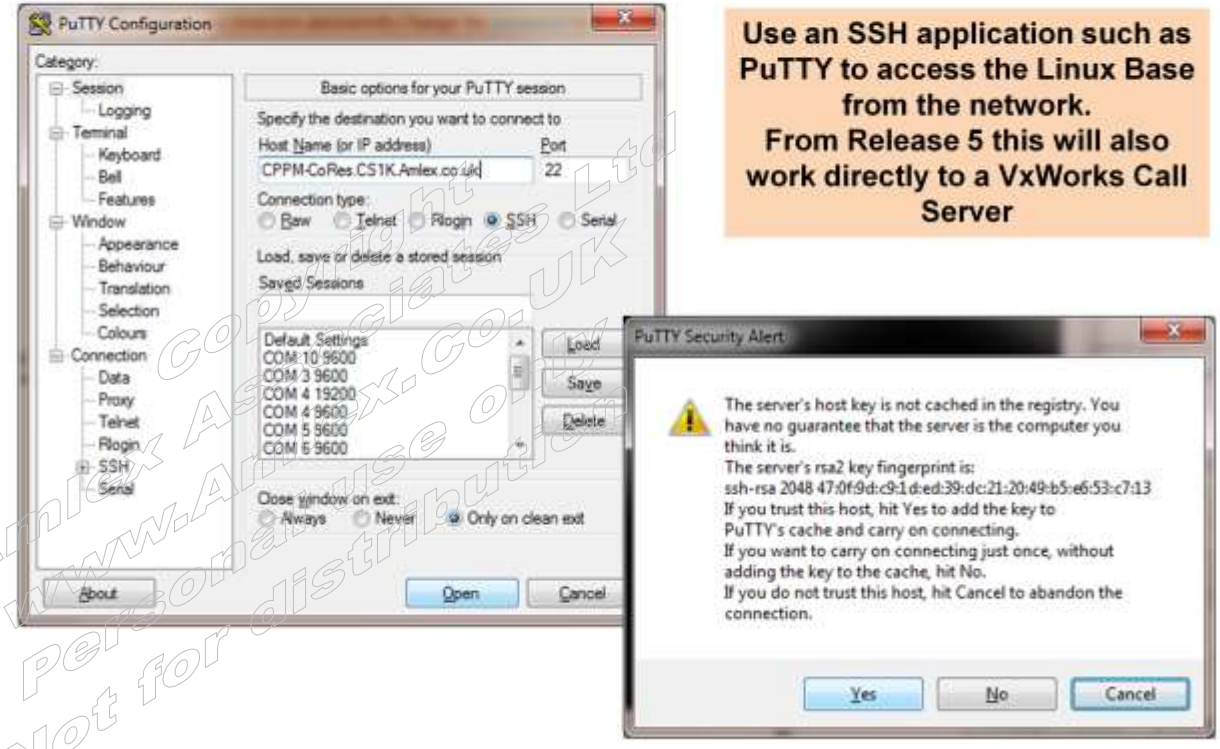
_____

_____

Use SSH to Login to Linux Server

Because SSH is a secure connection it will exchange a host key or Fingerprint when it connects to ensure the security of transmission.

As you can see here there is a challenge to accept the fingerprint of the server and cache it for future use.



Use an SSH application such as PuTTY to access the Linux Base from the network.
From Release 5 this will also work directly to a VxWorks Call Server

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

220

Notes

_____

_____

_____

_____

To access the overlays it depends on which type of machine we are connected to.

For a CoRes system i.e. Hosted on a Linux Base server we will need to login to the Linux command line first (Ideally using the “admin2 “ account). We then need to transition to the Call Server overlays and this is done using either
- csconsole (Preferred) or
-cslogin.

The reason csconsole is preferred is that it maintains the connection even when you detach using “<CTRL>ad” whereas cslogin will disconnect the session when the “~.” Command is used.

For an HA or SA system hosted on VXWorks the user will be placed directly into the overlays so no extra commands are required.

Access to Overlays

- CoRes Call Server
- From Linux CLI
  - csconsole
    - Connects to Console
    - <CTRL> ad - to exit
  - cslogin
    - Connects to Overlays
    - ~. – to exit
  - RLOGIN from network

- VXWorks Call server
  - e.g. High Availability dual cpu system
  - Any connection will take you directly into the Overlays
    - Direct from Console port
    - SSH to ELAN of Call Server
    - RLOGIN to ELAN

221

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

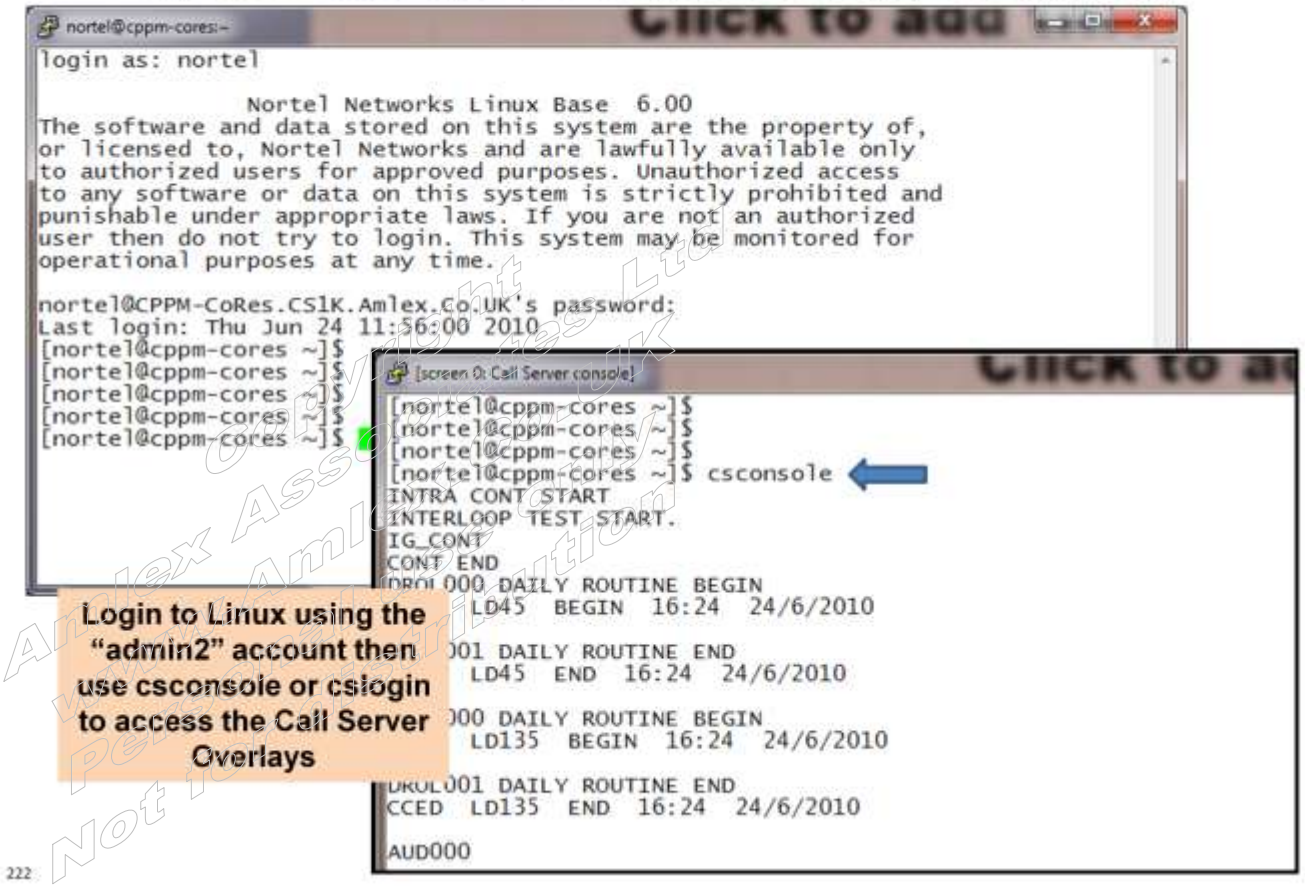
_____

_____

_____

Access to CoRes Call Server

The screenshots show an example of logging into the Linux server and then moving to the Call server Overlays using csconsole.


nortel@cppm-cores:~
login as: nortel
Nortel Networks Linux Base 6.00
The software and data stored on this system are the property of,
or licensed to, Nortel Networks and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.
nortel@CPPM-CoRes.CS1K.Amlex.Co.UK's password:
Last login: Thu Jun 24 11:56:00 2010
[nortel@cppm-cores ~]$
[screen 0: Call Server console]
[nortel@cppm-cores ~]$ csconsole
INTRA CONT START
INTERLOOP TEST START.
IG_CONT
CONT END
LD45 BEGIN 16:24 24/6/2010
LD45 END 16:24 24/6/2010
LD135 BEGIN 16:24 24/6/2010
LD135 END 16:24 24/6/2010
AUD000
Login to Linux using the "admin2" account then use csconsole or cslogin to access the Call Server Overlays

Notes

_____

_____

_____

_____

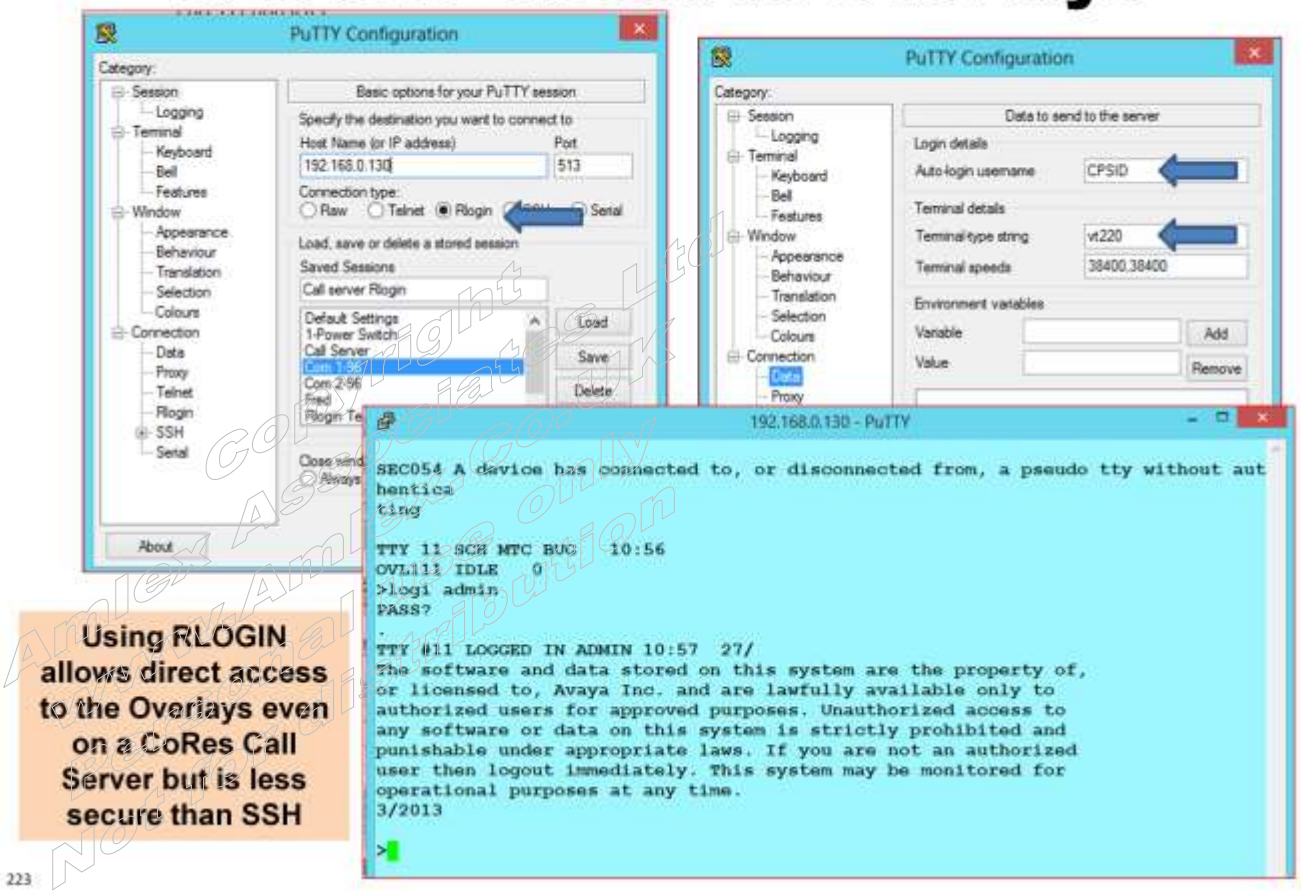
Copyright Amlex Associates Ltd

RLOGIN Direct to Overlays

Using RLOGIN is less secure than SSH but has the advantage of taking you directly to the overlays so can be less complex on a CoRes Call Server.

Set the RLOGIN client to point to the IP Address of the server ensuring that the port is set to 513. In this example we are using PuTTy and to jump directly to the Overlays you will need to select the DATA option under CONNECTION and then set the AUTO-LOGIN USERNAME to CPSID and the TERMINAL TYPE STRING to vt220.

On opening the connection you should be presented with a screen as shown at the bottom of the slide where you can use the normal login process.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

No ELAN configuration is required on the CoRes Call Server as it utilises the networking arrangements of the Linux server hosting it.

All of our IP configuration was done directly to the Linux Server so we do not need to add anything here as we would with a Standard or High availability system running VxWorks.

The next page shows how we can add one or two IP addresses for either a SA or HA VxWorks call server.

If it is a High Availability system we need two IP addresses, one for each call server, the Active address and the Inactive address. These are swapped between the two call servers (Side 0 and Side 1) as they change from being the active call server to the standby.

ELAN Configuration- CoRes

```
>
OVL000
>ld 117

OAM000

=> prt host

Command not Supported on Linux Call Server, please use "Base Manager" instead.

=> new host CS_ACT 10.10.10.130

Command not Supported on Linux Call Server, please use "Base Manager" instead.

=> stat host

Command not Supported on Linux Call Server, please use "Base Manager" instead.

=>
```

NOTE:- All of the IP Addresses are inherited from the Linux sever the system is hosted on.
Thus there is no requirement to set the IP Address of the Call server in Overlay 117.

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

224

Notes

_____

_____

_____

_____

Virtual Trunks are used to carry VoIP calls between systems without the need for conventional circuits just using IP networks.

This diagram shows the basic flow for a Virtual Trunk IP to IP call. Set 1000 is calling set 2000.

Set 1000 signals the call server via TPS on the Sig Server

Call server identifies 2000 as a remote set and sends the call to the Virtual trunk gateway (SIP or H.323) on Sig Server.

Sig server sends request to NRS (Network Routing Service) or Session Manager in and Aura installation, to identify where 2000 is.

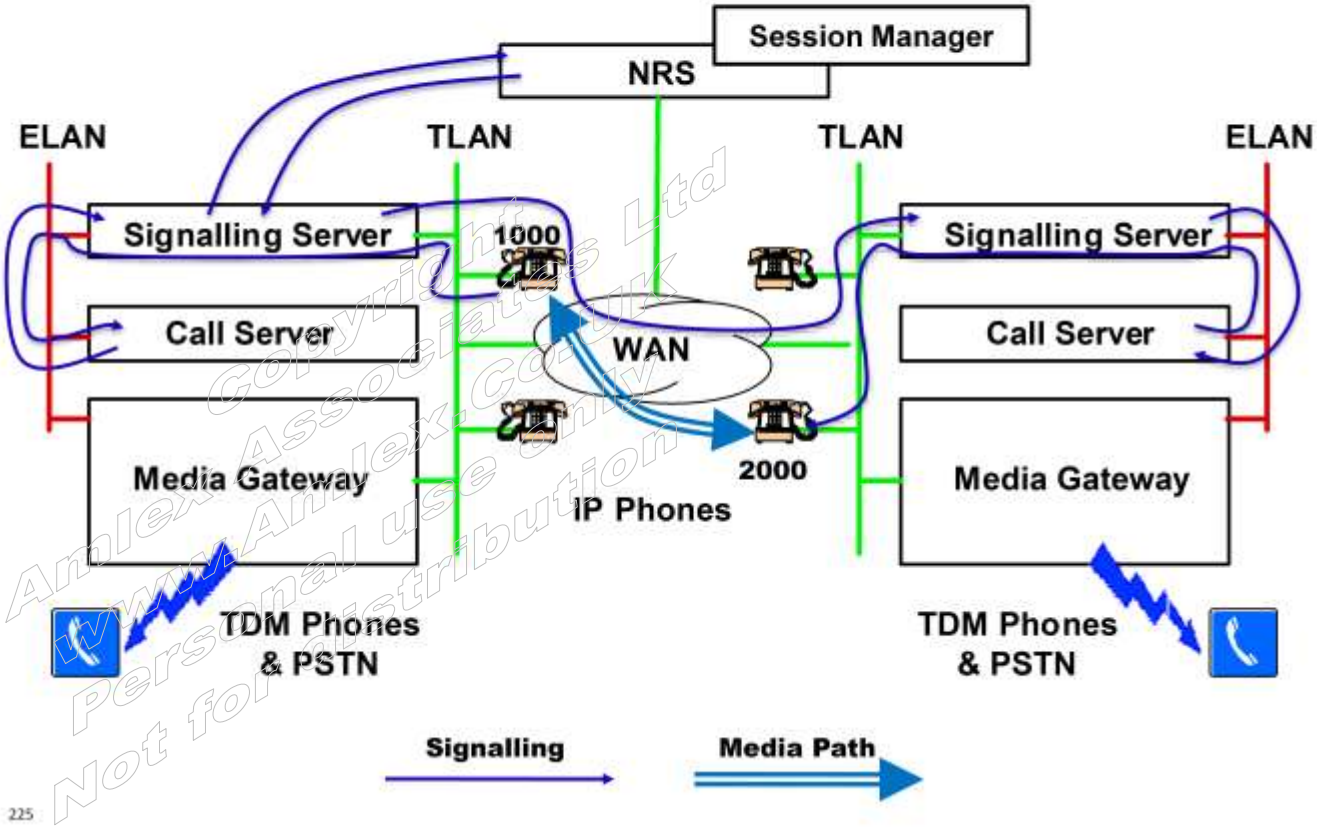
NRS responds with the IP address of the destination Signalling gateway.

The Signalling gateway on the initiating system then contacts the Signalling gateway on the destination system.

Request is sent to the CS on destination as an inbound D-Channel.

CS looks up set 2000 and then sends a call setup to it via the TPS on its Signalling server.

21. IP Virtual Trunks



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Both H.323 and SIP are available on CS1K to create Virtual Trunks.

SIP was introduced at Release 4 but is now the preferred option and more development has been done in Release 5 and 6 Much of this is relates to the integration with Microsoft OCS and Session Manager. Session Manager only supports NCS and SIP.

SIP is seen as the future direction and the addition of the SIP Line gateway and SIP trunks underline this.

SIP uses either a SIP Redirect Server or SIP Proxy Server to route calls between endpoints. On the NRS this is selected at configuration time however the Session Manage only works as a SIP Proxy.

H323 uses a Gatekeeper to route its calls between endpoints.

SIP & H.323

- H.323
  - Telephony Standard
  - Originates from Video Conf.
- Less flexibility
  - Written in ASN1
  - Difficult to Adapt
- Mature
  - Many H.323 G/W
- Up to 1200 H.323 Trunks per Sig Server

- SIP
  - Session Initiation Protocol
  - IETF standard
  - Domain based
- Flexible and Extensible
  - Additions can be made
  - "HTML of Telephony"
  - Text Based messages
- Microsoft Support
  - OCS uses SIP
- Up to 1800 SIP Trunks per Sig Server

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

226

Notes

_____

_____

_____

_____

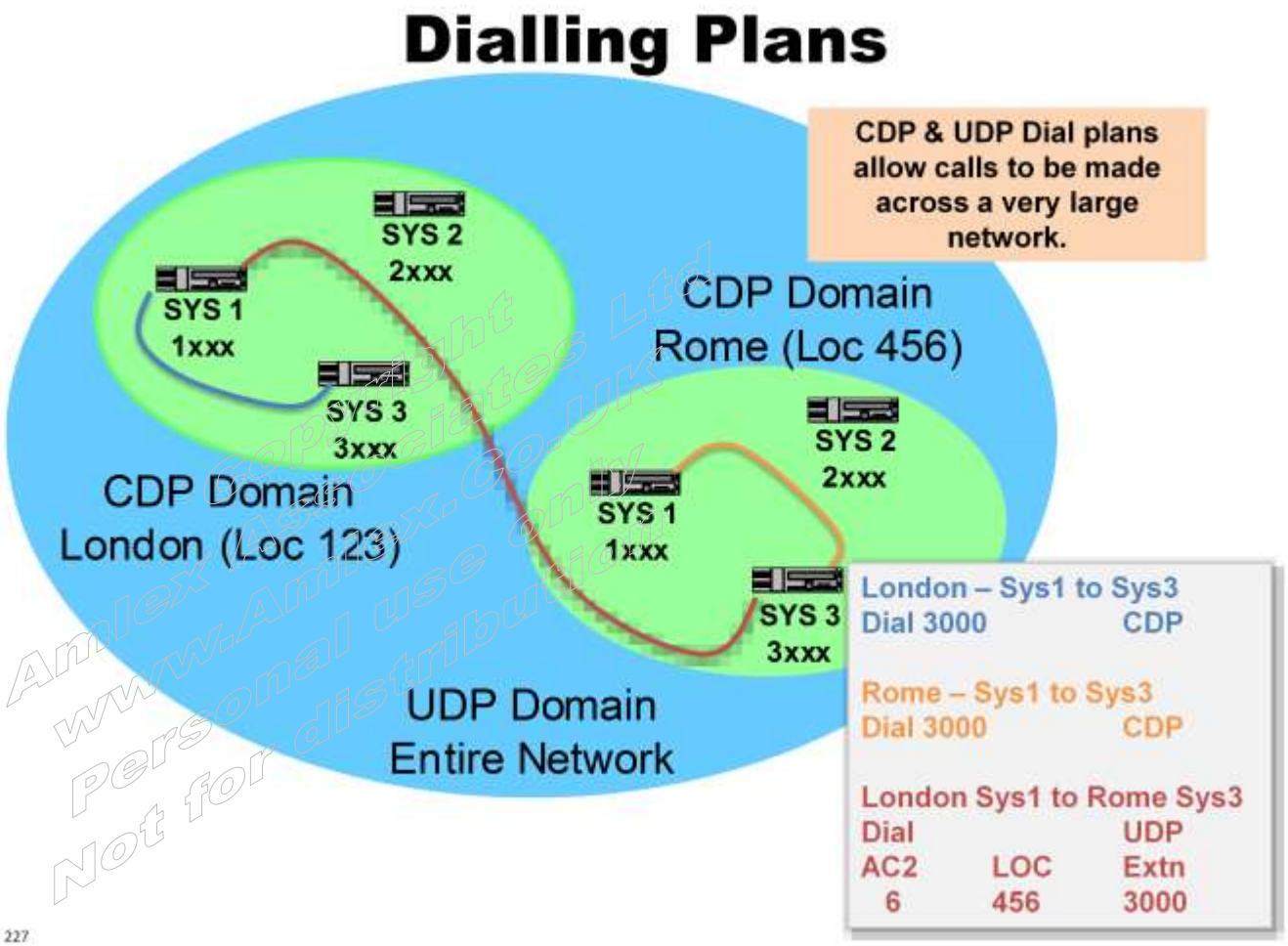
There are two main types of Dial Plan used on Nortel systems, these are :-

CDP **Co-ordinated Dial Plan**
UDP **Uniform Dial Plan**

CDP is the most common dial plan used in Meridian/CS1000 networks and allows users purely to dial the Extension number of any other user on the network.

However on a large network this can limiting due to the numbers in use and to accommodate larger networks we have UDP.

UDP adds extra digits into the Dial stream to identify different locations. As you can see from the diagram calling sets within the CDP domain is fine and only the Extension number is required. However calling from London to Rome needs extra digits to make the numbers unique. Thus we add a Location code for each different area. To tell the system we are using a Location code so it knows where to look in its Routing tables, we prefix the Location with an AC (Access code) usually AC2.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

When we use SIP in the Call server to communicate with other systems we need to take into account its Domain structure.

SIP uses the context or Universal Resource Identifier (URI) to define call destinations and source points. The URI is a Domain based construct and is used either alone or in conjunction with a phone number to uniquely define a destination.

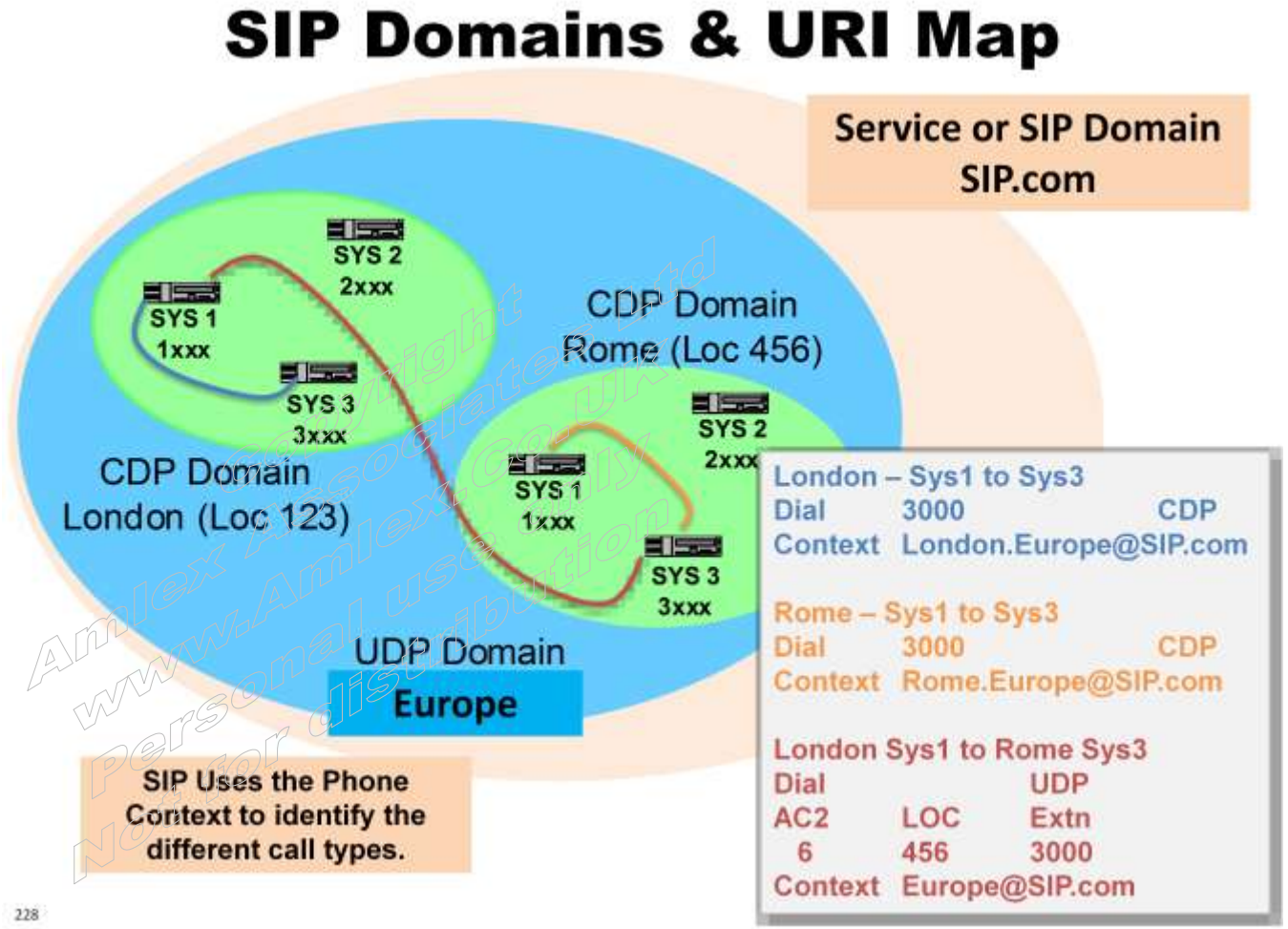
Within the CS1K we map the URI concept to both the Call Server IP Node as well as the NRS and use it to route calls.

In the diagram you can see how the three level structure is mapped to the CS1K dial plans

- ❑Service or SIP Domain
- ❑L1 Domain (UDP)
- ❑L0 Domain (CDP)

In this way we can handle CDP and UDP dial plans using SIP Virtual trunks.

In a Session Manager (Aura) configuration we use an Adaption to remove the CDP.UDP mapping to make it a generic SIP request.



Notes

_____

_____

_____

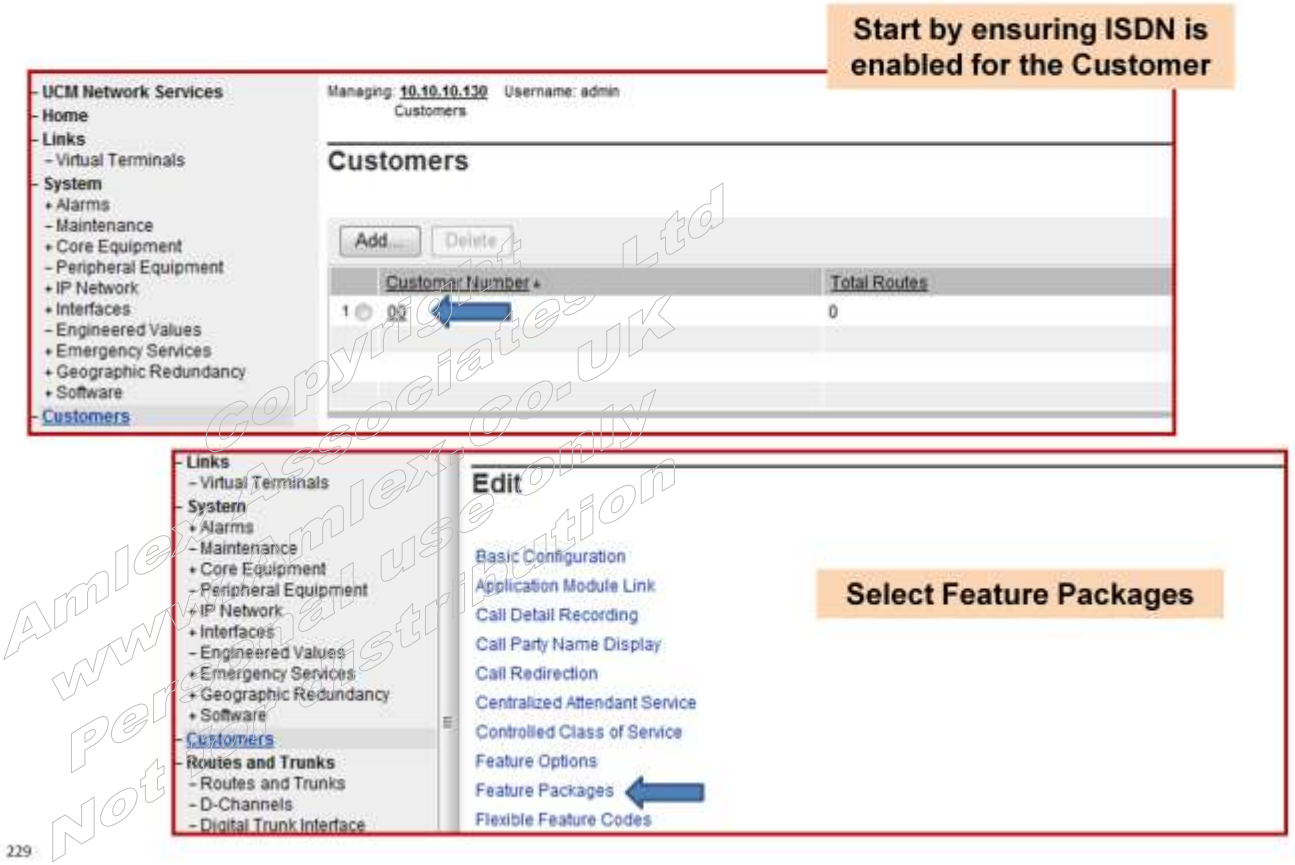
_____

Copyright Amlex Associates Ltd

Add ISDN Package

To use the Virtual trunks we must first of all enable ISDN on the system as our signalling to the Gateway will use this.

In Element Manager select the **CUSTOMER** option and then click on customer 00 and then the **FEATURE PACKAGES.**



Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

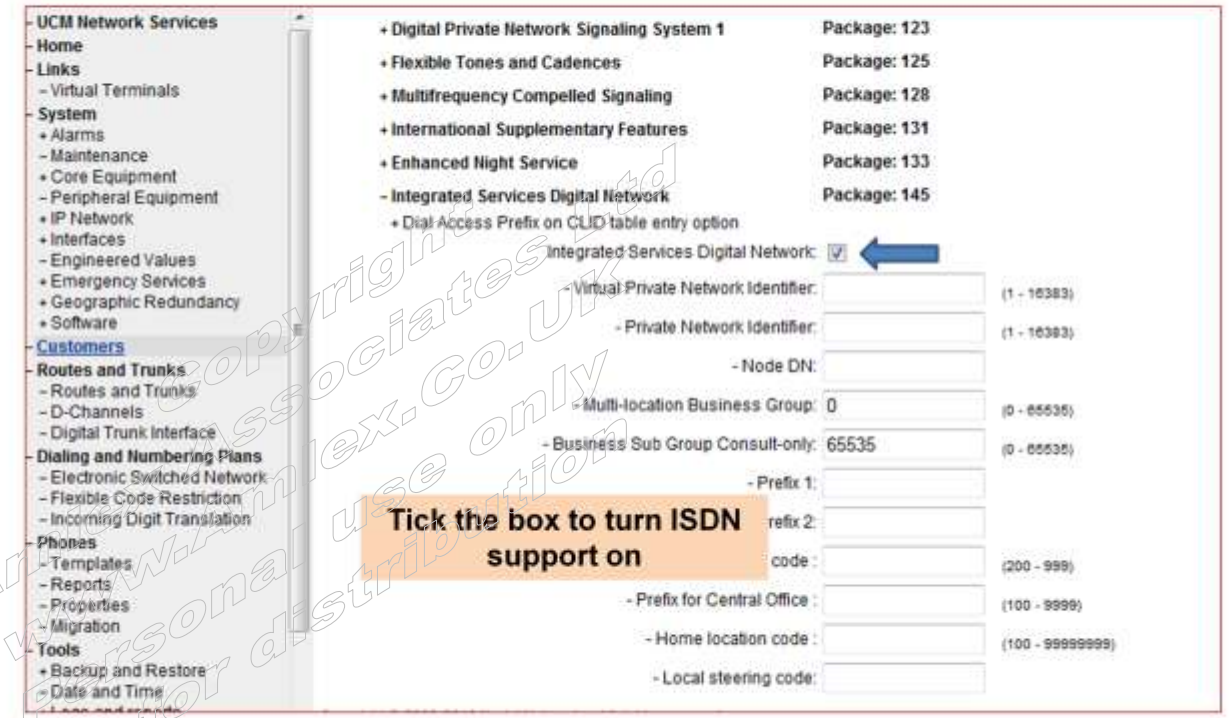
_____

Copyright Amlex Associates Ltd

Add ISDN Package

ISDN is Package 145 and when clicked on it will expand to show the tick box to enable it as well as options for VPNI and PNI etc.

At this point all we need to do is to enable the package.



Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

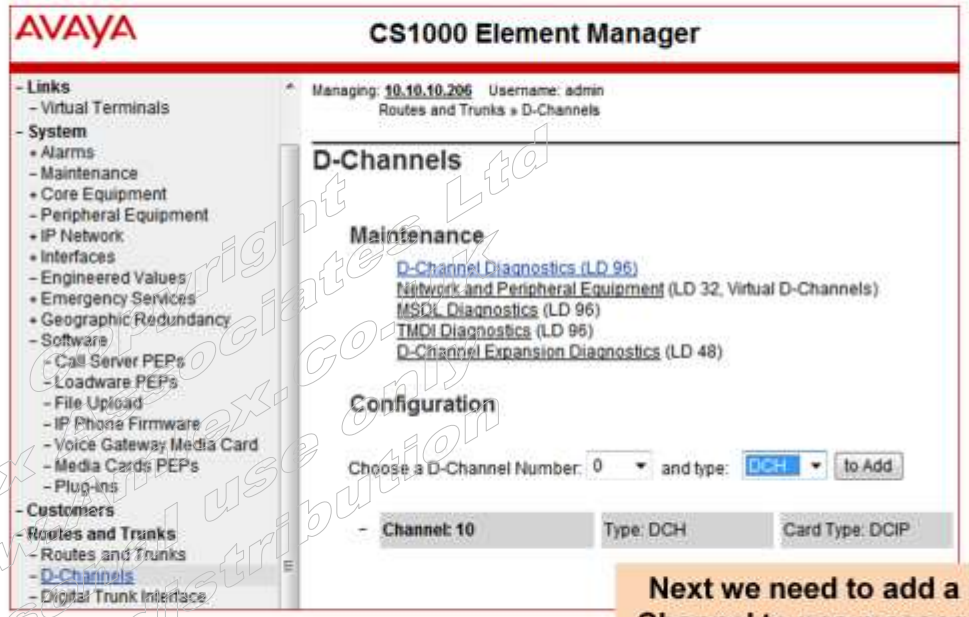
_____

Copyright Amlex Associates Ltd

Add Virtual D- Channel

We need to create a Virtual D-Channel for the Virtual Trunks. Navigate to the D-Channel screen and select the DCH number to add.

This D-Channel can be used for all IP Trunks even if you are running both SIP & H.323 Trunks. The Channel ID number configured on the Trunks themselves will identify exactly which to use.



Next we need to add a D Channel to pas messages to the Virtual Trunk Gateway on the signalling Server

Amlex Copyright www.amlex.co.uk Personal use only Not for distribution

231

Notes

_____

_____

_____

_____

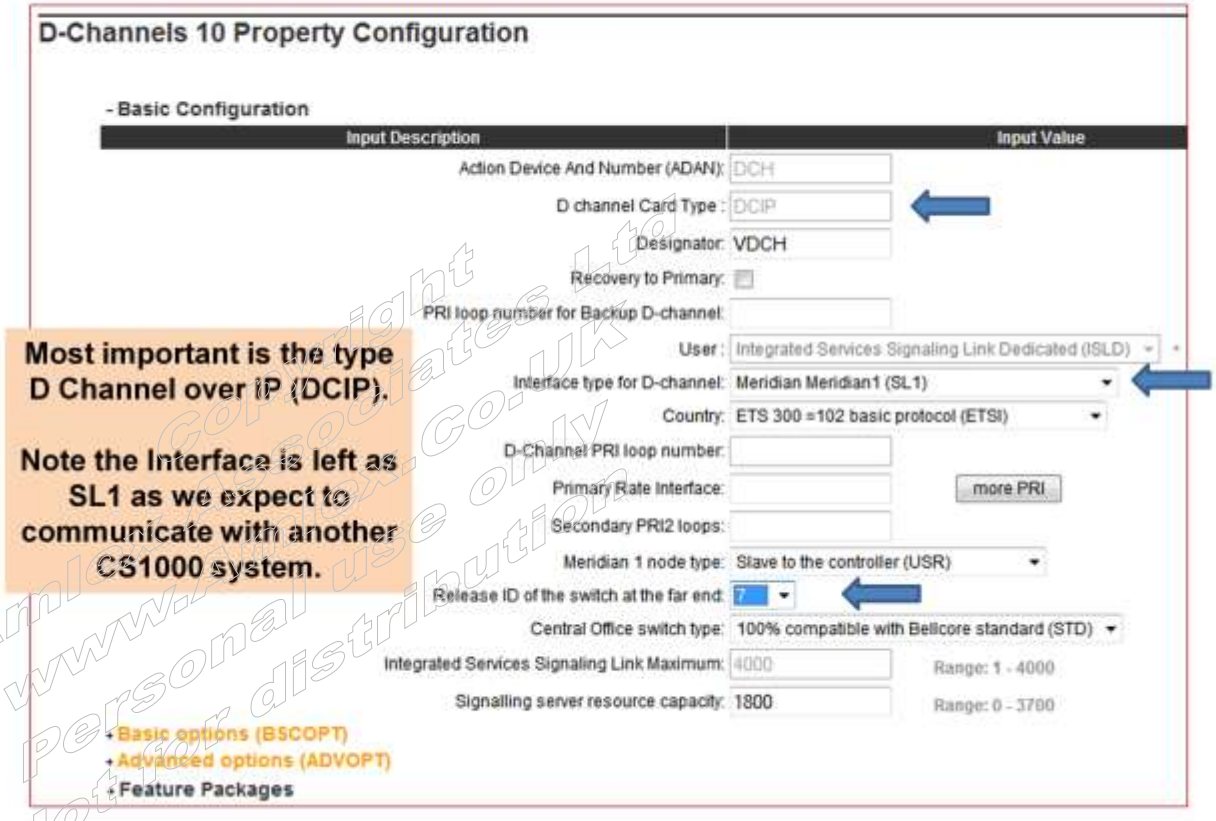
Copyright Amlex Associates Ltd

D-Channel over IP

The D-Channel type will be DCIP (D-Channel over IP) as messages will be passed over the ELAN to the Signalling Gateway

Select the **USER** as ISLD and the interface (**IFC**) as **MERIDIAN 1 (SL1)** as we will be sending MCDN over the IP Peer trunks.

Finally select the release ID for the far end **(RLS)** as **7**. This ensures the switch send compatible information.


D-Channels 10 Property Configuration
- Basic Configuration
Input Description
Input Value
Action Device And Number (ADAN): DCH
D channel Card Type : DCIP
Designator: VDCH
Recovery to Primary:
PRI loop number for Backup D-channel:
User : Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel: Meridian Meridian1 (SL1)
Country: ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:
Primary Rate Interface:
more PRI
Secondary PRI2 loops:
Meridian 1 node type: Slave to the controller (USR)
Release ID of the switch at the far end: 7
Central Office switch type: 100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum: 4000
Range: 1 - 4000
Signalling server resource capacity: 1800
Range: 0 - 3700
+ Basic options (BSCOPT)
+ Advanced options (ADVOPT)
+ Feature Packages
Most important is the type D Channel over IP (DCIP).
Note the Interface is left as SL1 as we expect to communicate with another CS1000 system.
232

Amlex Associates Ltd Copyright www.amlex.co.uk Personal use only Not for distribution

Notes

_____

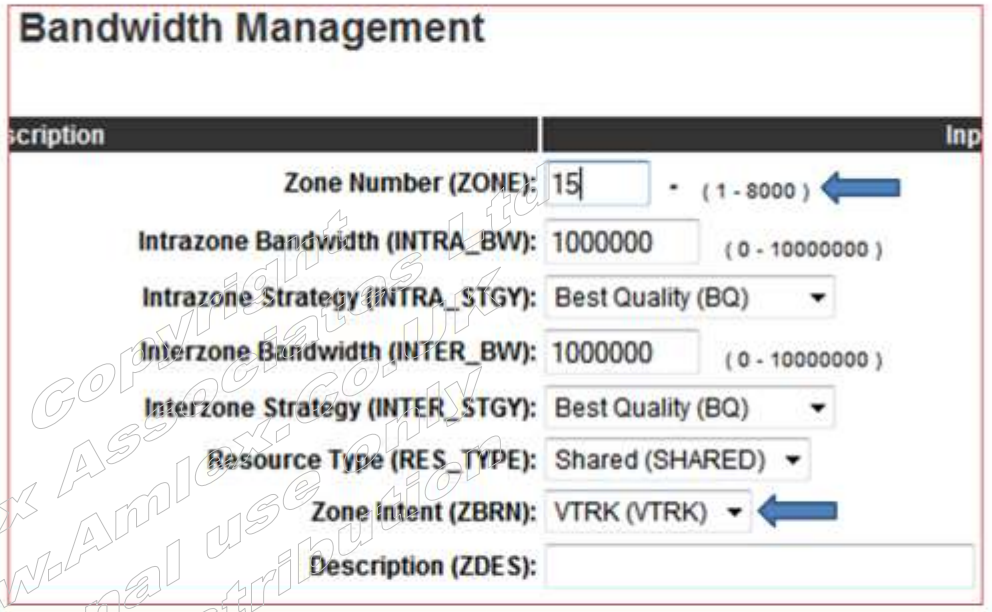
_____

_____

_____

Add VTRK Zone

Select the **SYSTEM / IP NETWORK / ZONES** option and add a virtual trunk route for the new Virtual trunk route. Adjust the bandwidth available to suit the links the trunks will use.


Bandwidth Management
cription
Inp
Zone Number (ZONE): 15 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW): 1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY): Best Quality (BQ)
Interzone Bandwidth (INTER_BW): 1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY): Best Quality (BQ)
Resource Type (RES_TYPE): Shared (SHARED)
Zone Intent (ZBRN): VTRK (VTRK)
Description (ZDES):

Add a new Bandwidth Zone with a ZONE INTENT (ZBRN) of VTRK

233

Notes

_____

_____

_____

_____

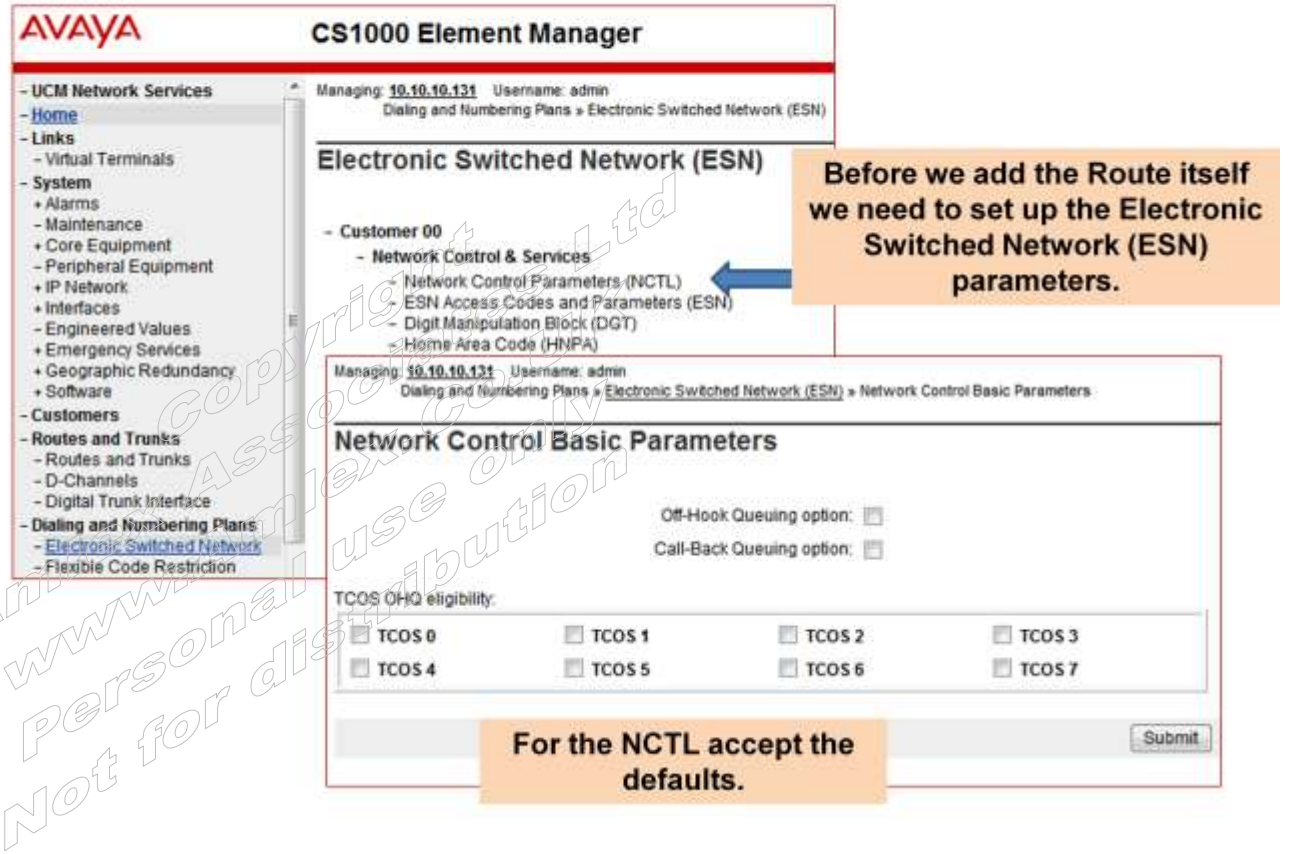
Copyright Amlex Associates Ltd

ESN – Network Control Basic Params

To allow us to programme Steering codes etc we need to create the default Electronic Switched Network tables. In Release 7 the system will not allow the creation of Routes before an ESN data lock is in place.

ESN allows us to create the Route list index, steering codes and access codes and perform complex routing.

Use the default values for Network Control Basic Parameters for our example and **SUBMIT**.



234

Notes

_____

_____

_____

_____

Amlex Associates Ltd Copyright
www.amlex.com
Personal use only
Not for distribution

We need to setup the ESN Access Codes and Parameters to dimension the system i.e. How many Steering Codes are allowed etc.

Set all values that are “Maximum....” to 100 except Maximum Number of Common Carriers which should be 0.

There are two Access Codes available on the system designated AC1 and AC2. They are used in the dialling schemes NARS (Network Alternate Routing system) and BARS (Basic Alternate Routing system).

In essence when one of the two AC codes is dialled the system selects only the Dial Plan information related to that Access code which might be a Special Number Code, a Location Code or Numbering Plan Area Code etc.

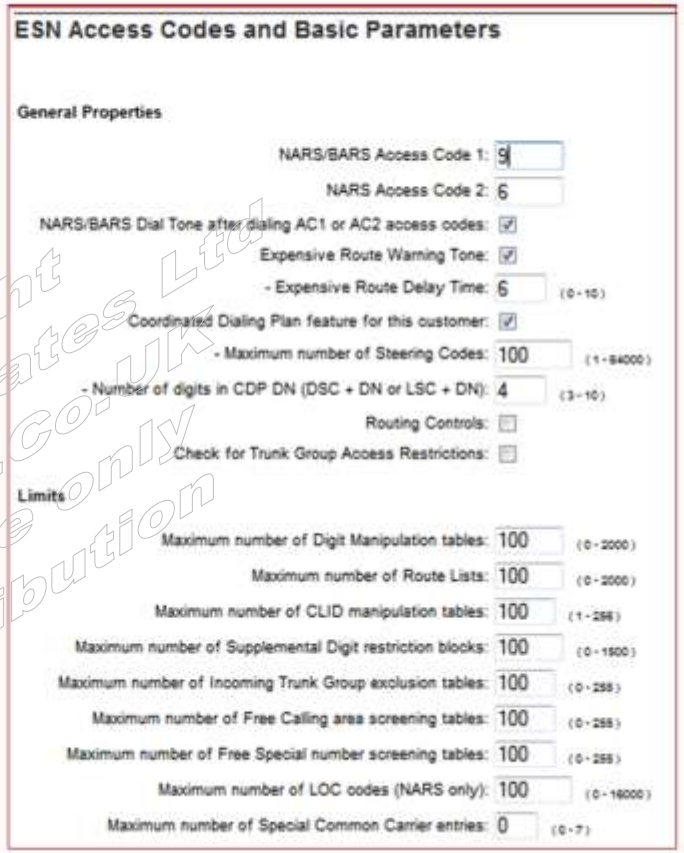
Set AC1 to 9 and AC2 to 6.

Finally set the number of digits in CDP DN to 4 as we are using 4 digit extension numbers in this example.

ESN Codes & Basic Parameters

Here we are dimensioning the table to ensure the system knows about the different codes etc.

AC1 = 9
AC2 = 6
Digits in CDP = 4
Maximum no ... = 100
Max. No. Special Common Carriers = 0


ESN Access Codes and Basic Parameters
General Properties
NARS/BARS Access Code 1: 9
NARS Access Code 2: 6
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes:
Expensive Route Warning Tone:
- Expensive Route Delay Time: 6 (0-10)
Coordinated Dialing Plan feature for this customer:
- Maximum number of Steering Codes: 100 (1-64000)
- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3-10)
Routing Controls:
Check for Trunk Group Access Restrictions:
Limits
Maximum number of Digit Manipulation tables: 100 (0-2000)
Maximum number of Route Lists: 100 (0-2000)
Maximum number of CLID manipulation tables: 100 (1-256)
Maximum number of Supplemental Digit restriction blocks: 100 (0-1500)
Maximum number of Incoming Trunk Group exclusion tables: 100 (0-255)
Maximum number of Free Calling area screening tables: 100 (0-255)
Maximum number of Free Special number screening tables: 100 (0-255)
Maximum number of LOC codes (NARS only): 100 (0-16000)
Maximum number of Special Common Carrier entries: 0 (0-7)

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

235

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add Route

Select the option **ROUTES AND TRUNKS / ROUTES AND TRUNKS** from the Element Manager menu. Then click the **ADD ROUTE** button to create the Virtual Trunk route.

Add a Route for the Virtual Trunks Note: - There are currently no routes on this system as it used the Default Database

Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

236

Notes

_____

_____

_____

_____

Configure SIP Route

The Configuration of the SIP route is as shown here.

Route Number (**ROUT**) A number

Designator (**DES**) Description

Trunk Type (**TYTP**) TIE

Incoming/Out (**ICOG**) IAO

Access Code (**ACOD**) A Number

Bandwidth Zone (**ZONE**) VTRK zone number

Node ID (**NODE**) Node ID of signalling g/w

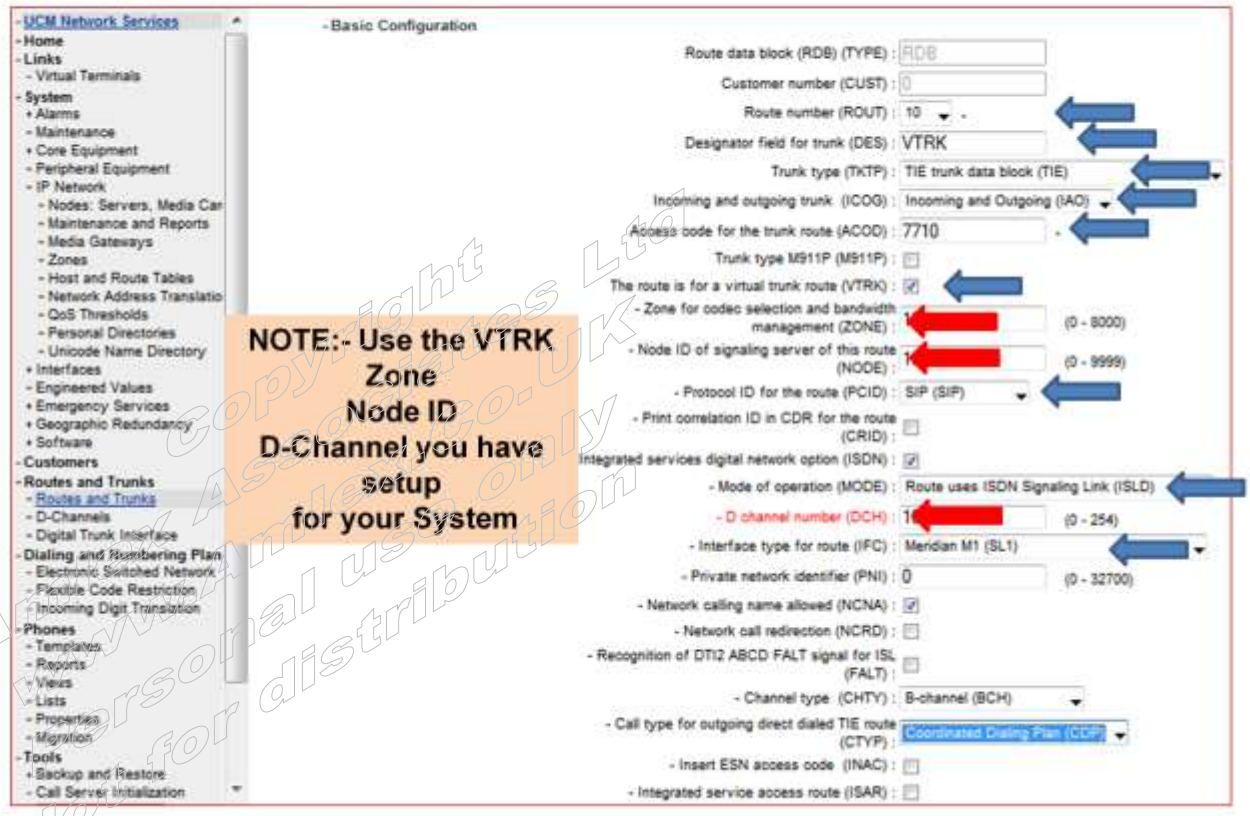
Protocol (**PCID**) SIP or H323

ISDN (**ISDN**) Tick

Mode (**MODE**) ISLD

Interface (**IFC**) Meridian SL1

Continued.....


- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 0
Route number (ROUT) : 10
Designator field for trunk (DES) : VTRK
Trunk type (TKTP) : TIE trunk data block (TIE)
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7710
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) : (0 - 8000)
- Node ID of signaling server of this route (NODE) : (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) :
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) : (0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 0 (0 - 32700)
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Coordinated Dialing Plan (CDP)
- Insert ESN access code (INAC) :
- Integrated service access route (ISAR) :
UCM Network Services
Home
Links
Virtual Terminals
System
Alarms
Maintenance
Core Equipment
Peripheral Equipment
IP Network
Nodes: Servers, Media Car
Maintenance and Reports
Media Gateways
Zones
Host and Route Tables
Network Address Translatio
QoS Thresholds
Personal Directories
Unicode Name Directory
Interfaces
Engineered Values
Emergency Services
Geographic Redundancy
Software
Customers
Routes and Trunks
Routes and Trunks
D-Channels
Digital Trunk Interface
Dialing and Numbering Plan
Electronic Switched Network
Flexible Code Restriction
Incoming Digit Translation
Phones
Templates
Reports
Views
Lists
Properties
Migration
Tools
Backup and Restore
Call Server Initialization
NOTE:- Use the VTRK Zone
Node ID
D-Channel you have setup
for your System
237

Copyright Amlex Associates Ltd
Personal use only
Not for distribution

Notes

_____

_____

_____

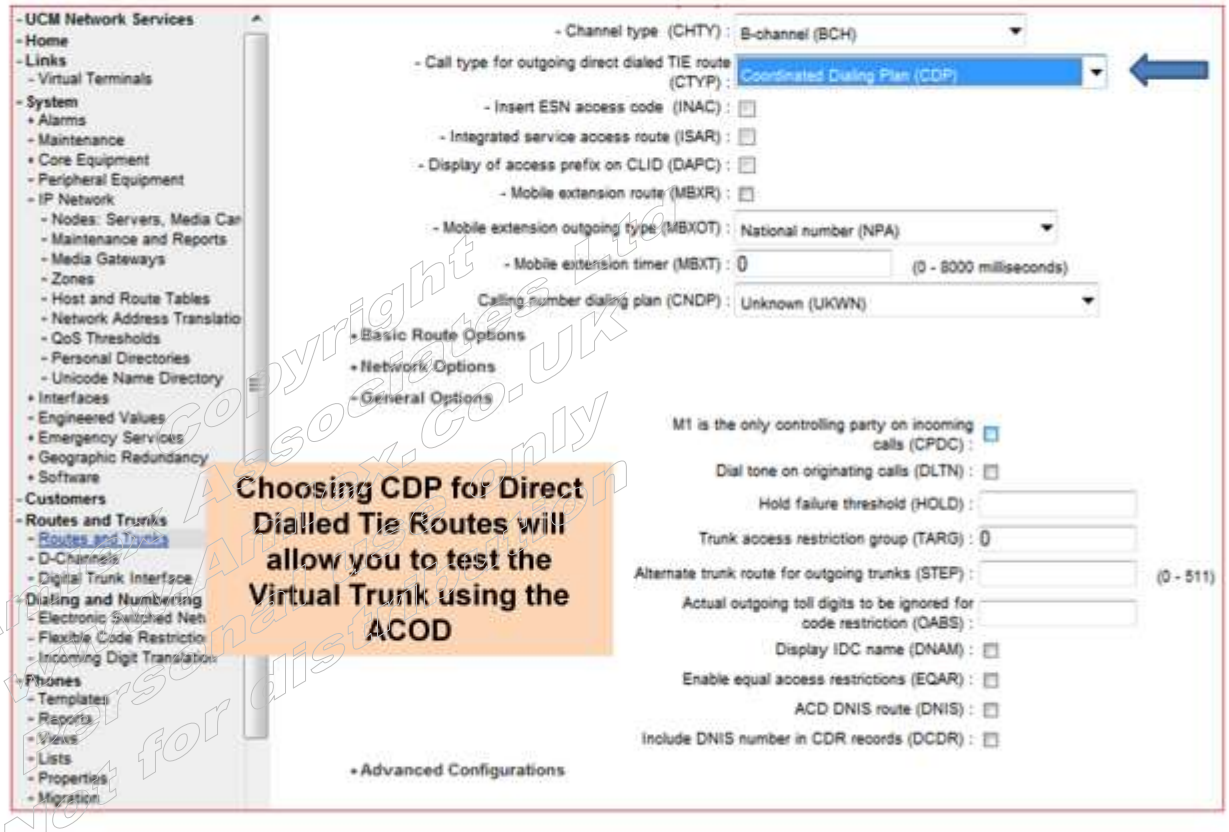
_____

Call Type & TARG

Call Type (**CTYP**) CDP

Trunk Acc Group (**TARG**) 1

Save the configuration ready to add the trunks.


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Car
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translatio
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering
- Electronic Switched Net
- Flexible Code Restrictio
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Coordinated Dialing Plan (CDP)
- Insert ESN access code (INAC) :
- Integrated service access route (ISAR) :
- Display of access prefix on CLID (DAPC) :
- Mobile extension route (MBXR) :
- Mobile extension outgoing type (MBXOT) : National number (NPA)
- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) : Unknown (UKWN)
+ Basic Route Options
+ Network Options
- General Options
M1 is the only controlling party on incoming calls (CPDC) :
Dial tone on originating calls (DLTN) :
Hold failure threshold (HOLD) :
Trunk access restriction group (TARG) : 0
Alternate trunk route for outgoing trunks (STEP) : (0 - 511)
Actual outgoing toll digits to be ignored for code restriction (OABS) :
Display IDC name (DNAM) :
Enable equal access restrictions (EQAR) :
ACD DNIS route (DNIS) :
Include DNIS number in CDR records (DCDR) :
+ Advanced Configurations
Choosing CDP for Direct Dialled Tie Routes will allow you to test the Virtual Trunk using the ACOD
238

Notes

_____

_____

_____

_____

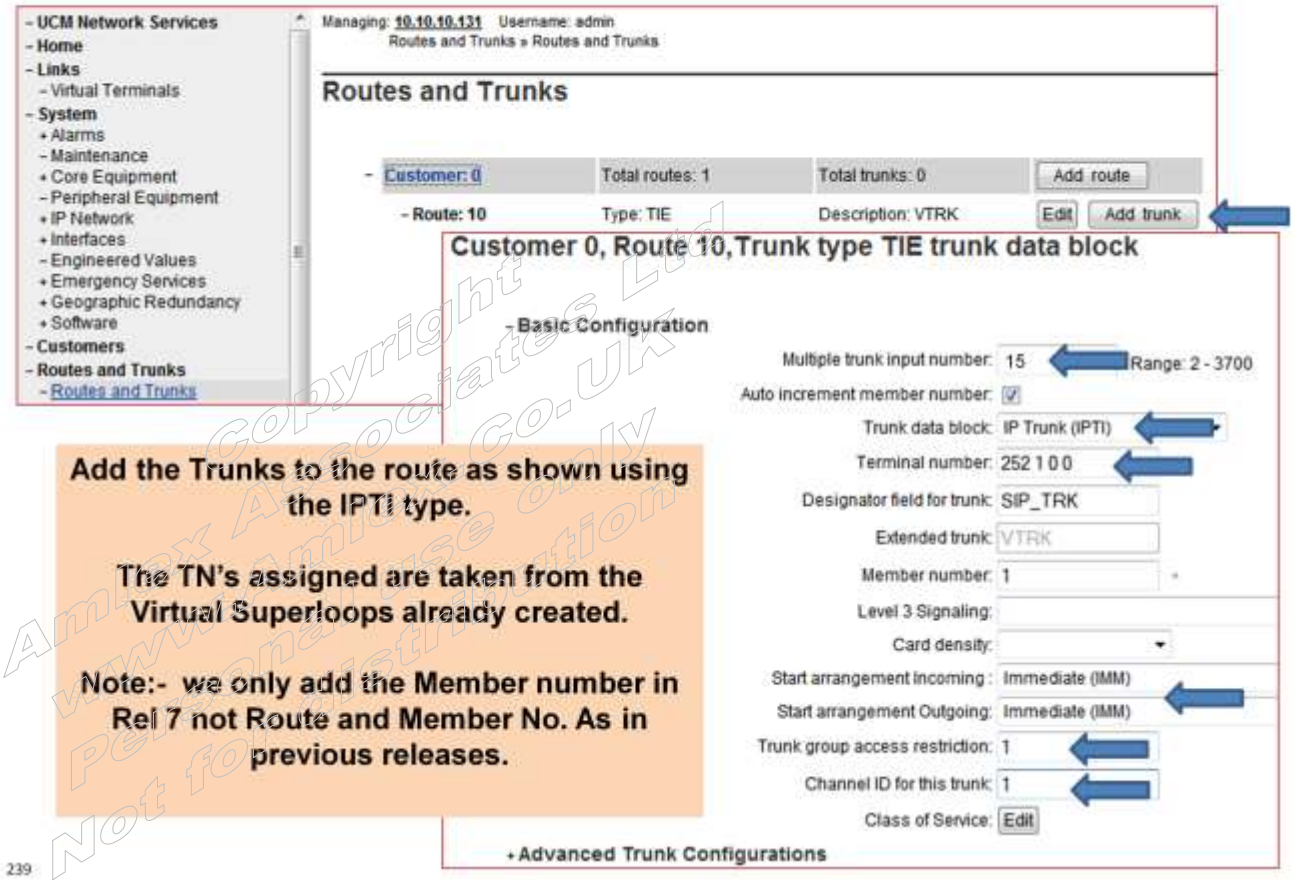
Copyright Amlex Associates Ltd

Add Trunks to Route

Add the trunks to the Route ensuring you have allocated enough Virtual TN's before starting.

Multiple input (**MTINPUT**)	15
Trunk Type (**TYPE**)	IPTI
Terminal No.(**TN**) Virtual TN's	
Designator (**DES**) Description	
Member No (**RTMB**)	1
Start Incoming (**STRI**)	IMM
Start Outgoing (**STRO**)	IMM
Trunk Group Res (**TGAR**)	1
Channel ID (**CHID**)	1

Save the trunks when completed.



Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Notes

_____

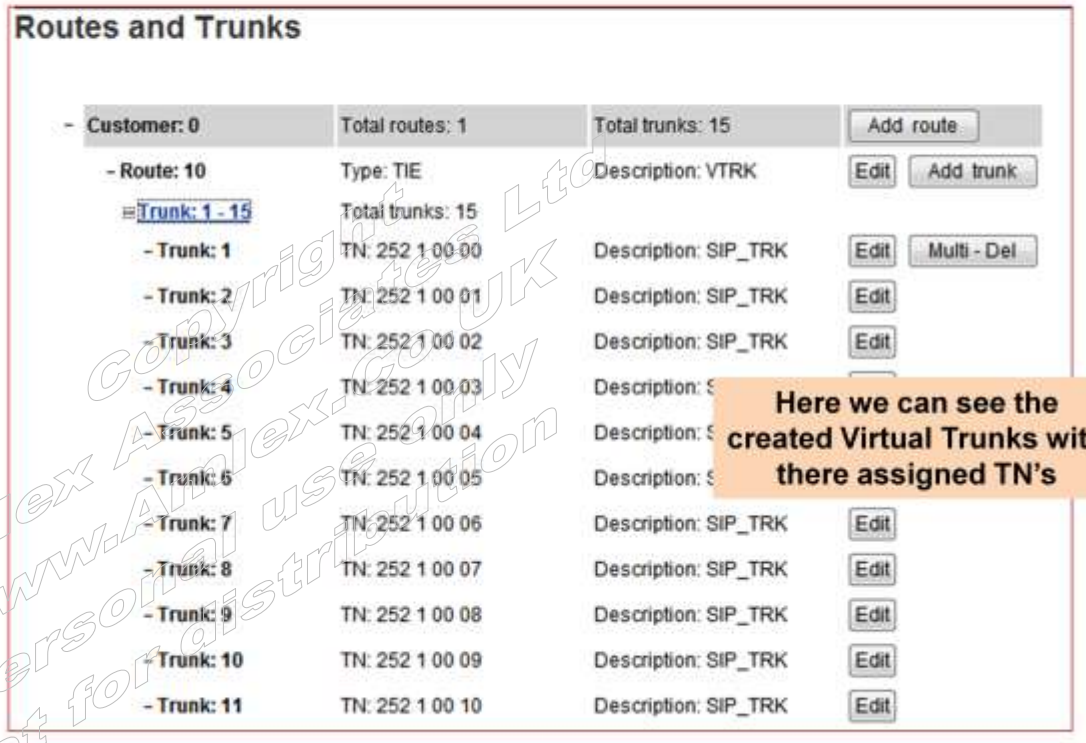
_____

_____

_____

Route & Trunks

The Virtual Route and Trunks are now completed and we can check to see if they are working .



Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

240

Notes

_____

_____

_____

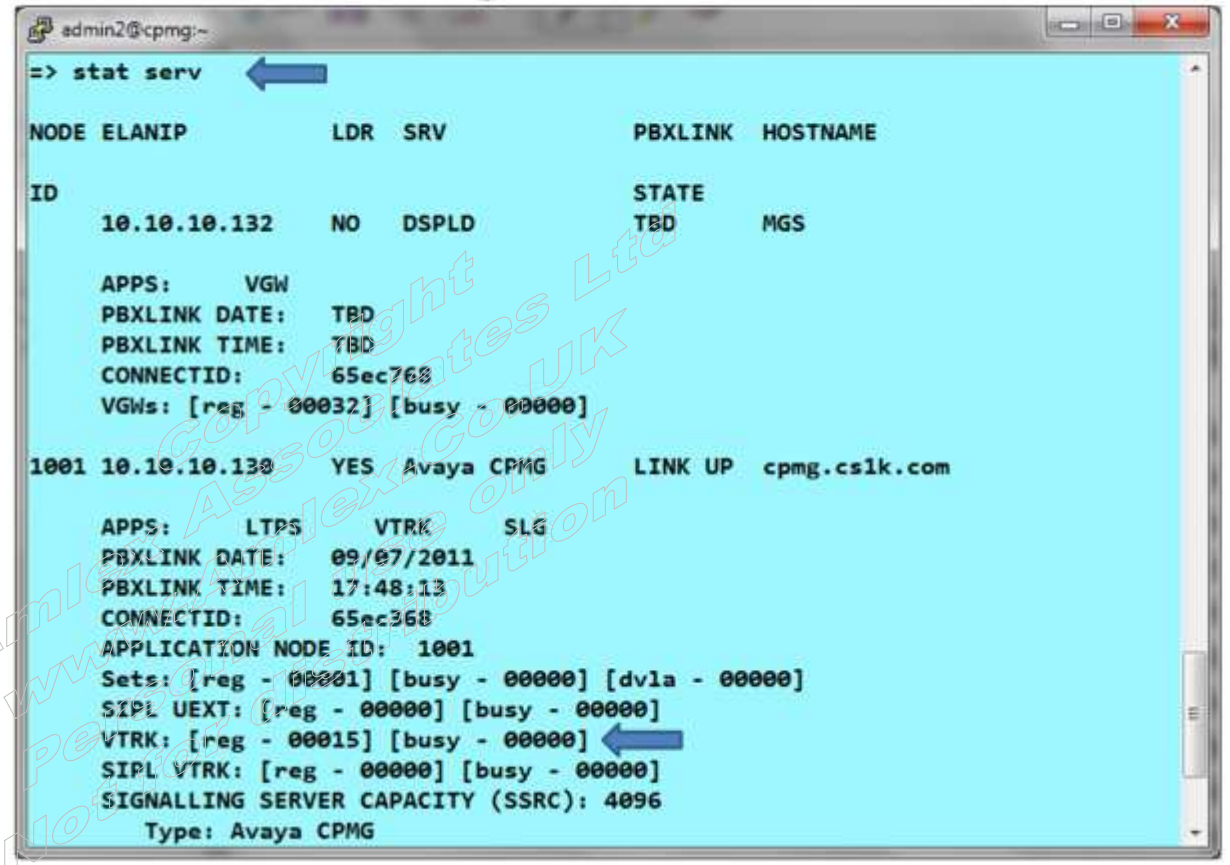
_____

Copyright Amlex Associates Ltd

Checking Virtual Trunks

Login to the Call Server and in LD 117 type STAT SERV as shown here to display the status of the Signalling Servers and Media Gateways.

Here you can see the Virtual Trunks registered and idle on the signalling server.


admin2@cpmg:~
=> stat serv
NODE ELANIP LDR SRV PBXLINK HOSTNAME
ID STATE
10.10.10.132 NO DSPLD TBD MGS
APPS: VGW
PBXLINK DATE: TBD
PBXLINK TIME: TBD
CONNECTID: 65ec768
VGWs: [reg - 00032] [busy - 00000]
1001 10.10.10.130 YES Avaya CPMG LINK UP cpmg.cs1k.com
APPS: LTPS VTRK SLG
PBXLINK DATE: 09/07/2011
PBXLINK TIME: 17:48:13
CONNECTID: 65ec368
APPLICATION NODE ID: 1001
Sets: [reg - 00001] [busy - 00000] [dvla - 00000]
SIPL UEXT: [reg - 00000] [busy - 00000]
VTRK: [reg - 00015] [busy - 00000]
SIPL VTRK: [reg - 00000] [busy - 00000]
SIGNALLING SERVER CAPACITY (SSRC): 4096
Type: Avaya CPMG
241

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Checking Virtual Trunks

Other options to check the Virtual trunk installation are shown here.

- LD 96 STAT DCH <DCH No.> checks the D channel is established.
- In the Linux CLI $SIPGwShow tSSG Shows the status of the Signalling gateway
- In the Linux CLI $vtrkShow Summary of Virtual Trunks

In The Overlays

```
>ld 96
DCH000
.
DCH000
.stat dch 10
DCH 010 : OPER     EST  ACTV AUTO      DES
     : VDCH
```

In LINUX Command Line

```
[nortel@cppm-cores ~]$ SIPGwShow tSSG

=== VTRK ===
SIPNPM Status                : Active
Primary  Proxy IP address    : 192.168.0.130
Primary  Proxy port          : 5060
Primary  Proxy Transport     : TCP
Secondary Proxy IP address   : 0.0.0.0
Secondary Proxy port         : 5060
Secondary Proxy Transport    : TCP
Active   Proxy               : Primary  :Not Registered
Time To Next Registration    : 12 Seconds
Channels Busy / Idle / Total : 0 / 15 / 15
Stack version                : 4.0.0.30
TLS Security Policy          : Security Disabled
SIP Gw Registration Trace    : OFF
Output Type Used             : RPT
Channel tracing              : -1
[nortel@cppm-cores ~]$
```

```
[nortel@cppm-cores ~]$ vtrkShow

=== VTRK ===


---------------------------
VTRK Summary

---------------------------
VTRK status   : Active
Master status : On
Protocol      : H323 SIP
D-Channel     : 10
Customer      : 0
Channels Idle : 15
Channels Busy : 0
Channels Mbsy : 0
Channels Pend : 0
Channels Dsbl : 0
Channels Ukwn : 0
Channels Total: 15
Chid ranges   : 1 to 15

VTRK State = Active
---------------------------

VTRK Status = Enabled
---------------------------
```

Amlex Copyright Associates Ltd www.amlex.co.uk Personal use only Not for distribution

242

Notes

_____

_____

_____

_____

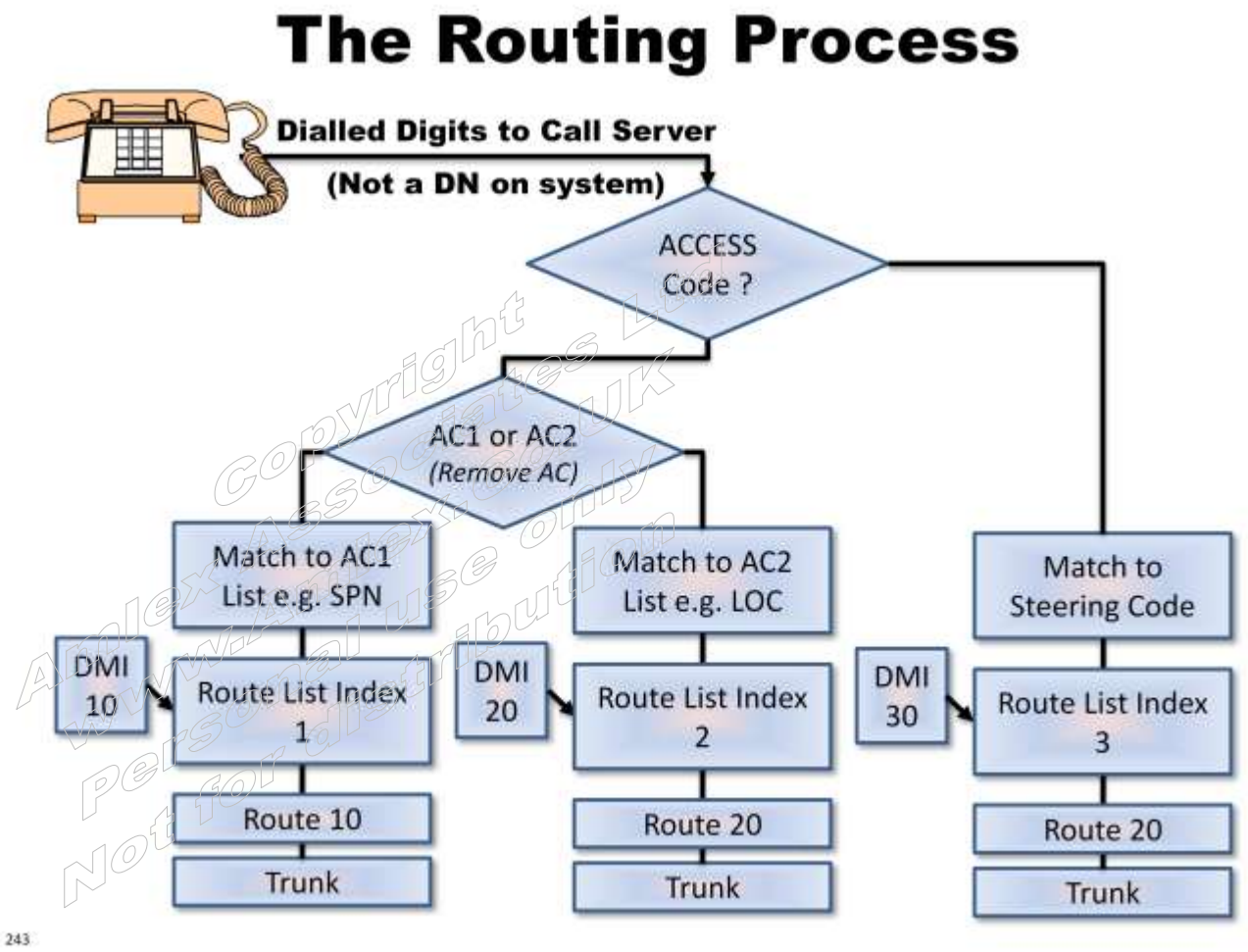
The Routing Process for a dialled number that isn't a DN on the systems is outlined here. Existing DN's could be Extensions, Hunt groups, Phantom numbers etc.
First the system checks whether an Access code (AC1 or AC2) has been dialled. If it has, it will firstly remove the AC code and then restrict its search for a match to the relevant list.

The subsequent match will also attach a Call Type to the call which is carried along with it.

If the first digit dialled is neither of the two AC codes then the system will search through the Steering codes (Distance, Local & Trunk) for a match again with a call type being added.

The generated match will point to a Route List Index, (RLI) this is a table which directs the call to the right Route off the system. It will also apply a Digit Manipulation (DMI) before forwarding to the route and finally the trunk.

The DMI will delete and insert digits as required .



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

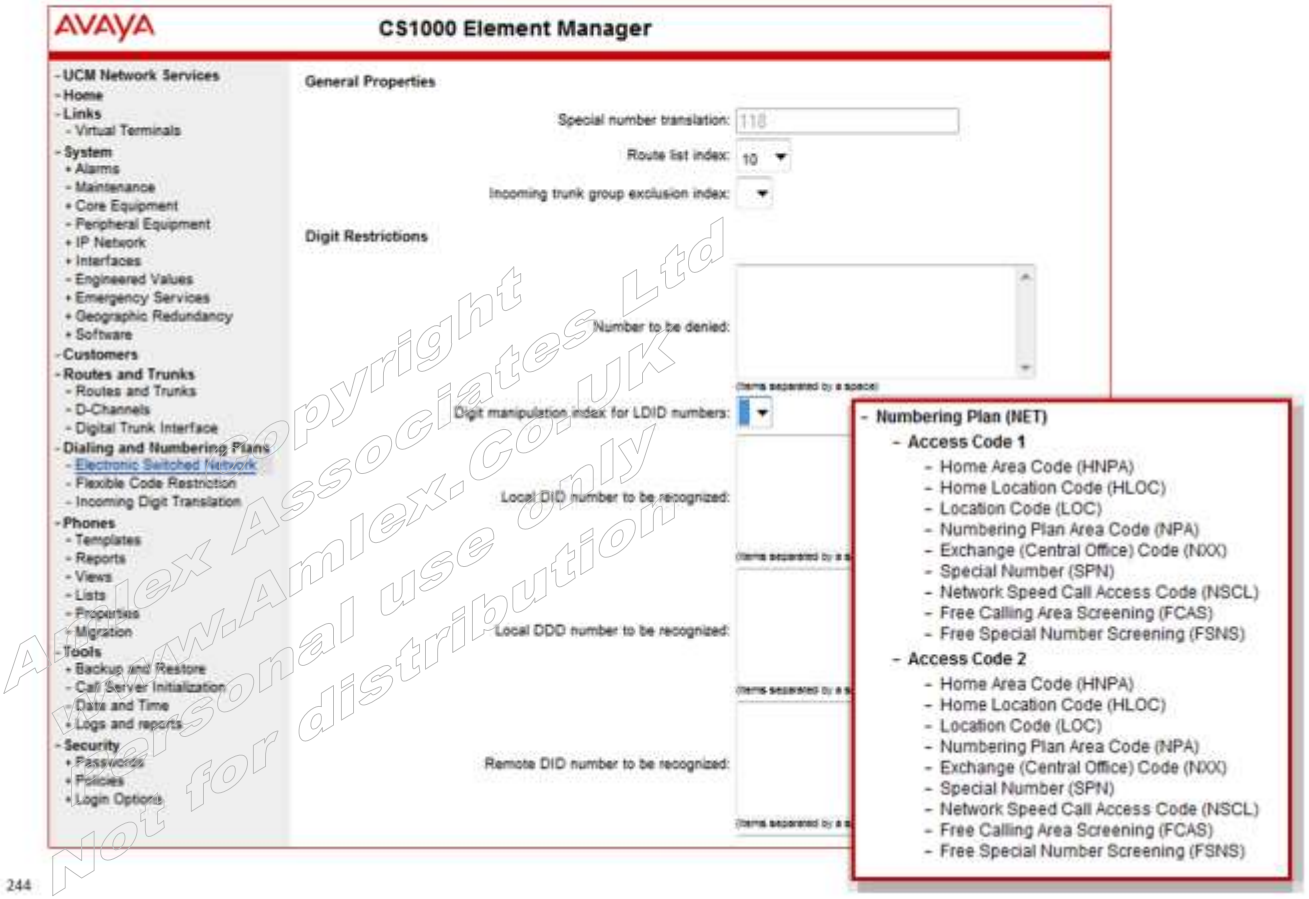
Access Codes

The figures show the dialogue for adding a Special Number to the ESN scheme. In this instance we are adding a local area code and then sending that out across RLI 10.

One point to note is the FLEN, Flexible Length. This is the number of digits expected before outpulsing to the network. If this is left at 0 then the system will wait for several seconds before sending the number. This can result in a long pause or Post Dial Delay as its sometimes known. To avoid this set the FLEN to the length of the number to be dialled.

The inset shows the list of codes which can be added under either an AC1 or AC2 code.

To create or edit codes in the overlays use LD 90 eg
LD 90
REQ new
CUST 0
FEAT net
TRAN ac1
TYPE spn
SPN 118



Amlex Copyright
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Route List Block

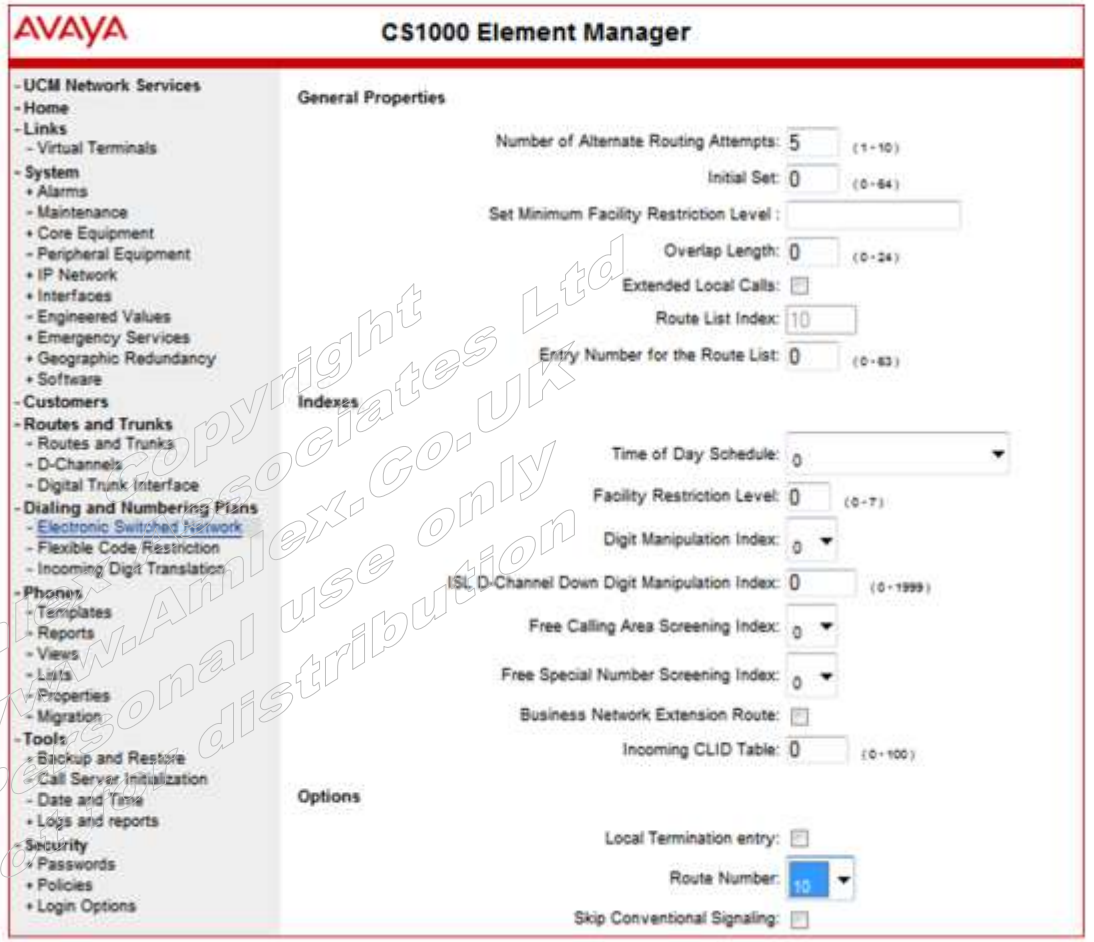
The Route List Block (RLB) contains the Route List Index (RLI) entries which are used to direct calls to the correct Route and apply the correct Digit Manipulation before out pulsing on the selected route.

In the figure you can see that RLI 10 is setup to send the calls to Route 10 using the default DMI 0 i.e. No changes.

Other options include Time of Day scheduling. Multiple entries can be made against the RLI so that if the first option is not available the second maybe used as a fallback.

By using multiple RLI's the same route can have many different types of calls routed across it using differing DMI's.

RLI's are created in overlay LD 86:-
>ld 86
REQ new
CUST 0
FEAT **rlb**
RLI 11
ENTR 0
LTER
ROUT 10
TOD
SCNV
CNV.....



Amlex Copyright
www.Amlex.Co.UK
Personal use only
No distribution

245

Notes

_____

_____

_____

_____

Digit Manipulation

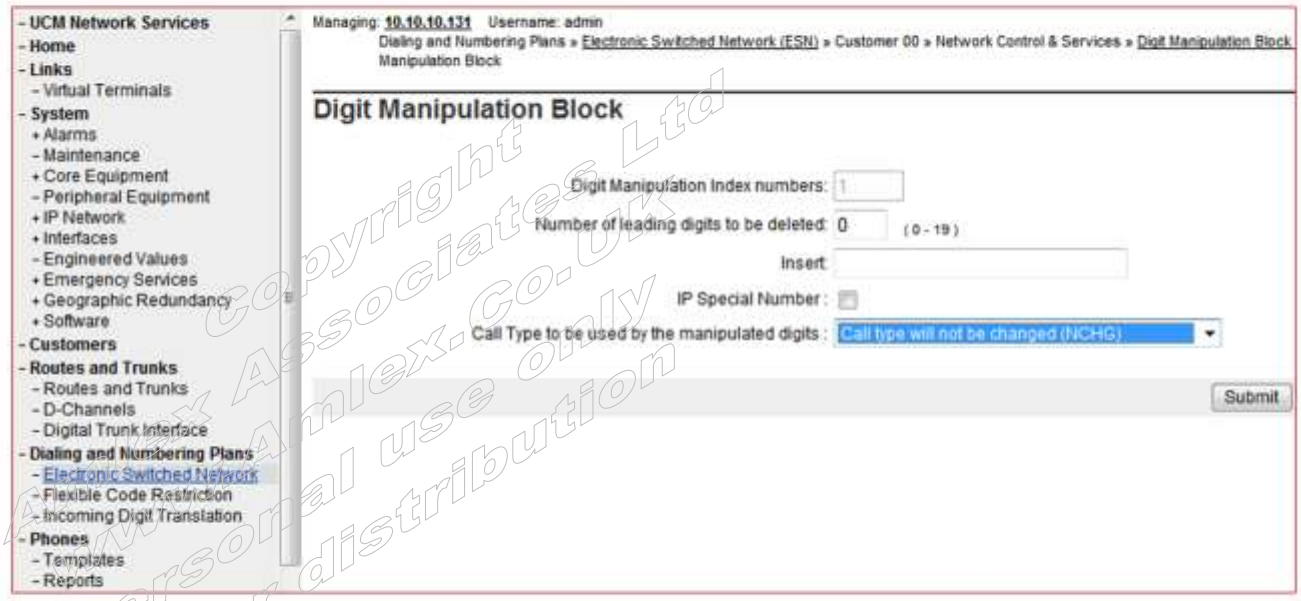
Digit Manipulation is the mechanism used to add, remove or replace digits in the dial string and also to change the call type.

The Default DMI is 0 which is set to Delete nothing, add nothing and not change the call type. This is not editable.

The figure opposite shows a DMI being added which deletes 3 digits but inserts nothing. The drop down menu shows the options for changing the call type if required.

To create a DMI in the overlays:-

>ld 86
REQ new
CUST 0
FEAT **dgt**
DMI 4
DEL 4
ISPN
INST 01234
CTYP cdp


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
Managing: 10.10.10.131 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block
Manipulation Block
Digit Manipulation Block
Digit Manipulation Index numbers: 1
Number of leading digits to be deleted: 0 (0 - 19)
Insert:
IP Special Number :
Call Type to be used by the manipulated digits : Call type will not be changed (NCHG)
Submit

Amlex Associates Ltd Copyright Personal use only Not for distribution

246

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Steering Codes

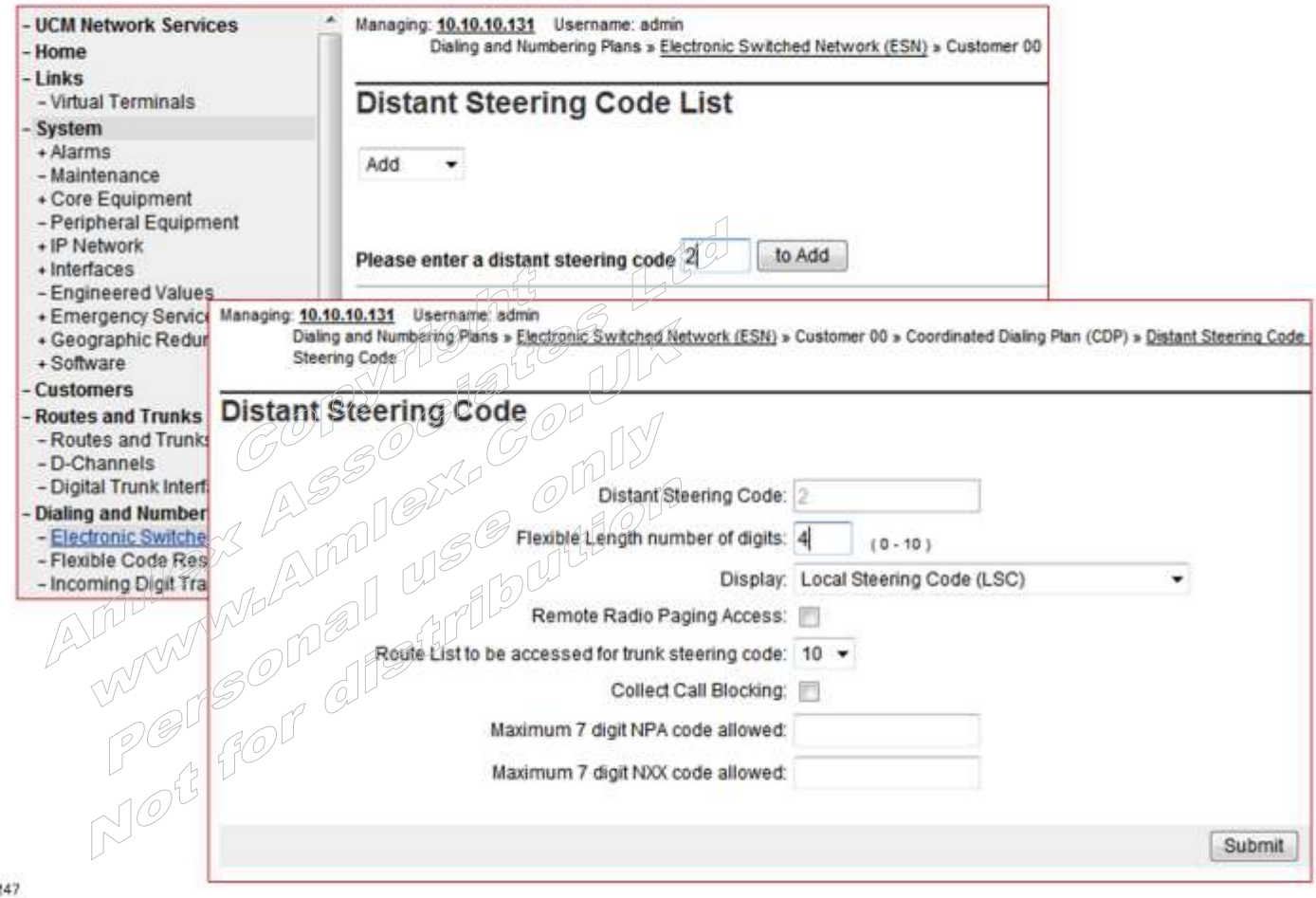
There are three types of Steering Code in the system, Local, Trunk and Distant, but these days the Distant Steering Code (DSC) is the one mainly used.

The DSC is used in CDP dialling to direct a call to a route using an RLI.

The DSC here is 2, and therefore any call dialled as a CDP number, starting with a 2 will be matched. The FLEN set is for so if someone dials 2000 on the system this DSC will pickup the call and forward it to RLI 10 for termination.

To add a Steering code in the overlays:-

>ld 87
REQ new
CUST 0
FEAT **cdp**
TYPE **dsc**
DSC 3
FLEN 4
DSP
RRPA
RLI 11
CCBA
NPA
NXX
DSC


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Servic
+ Geographic Redur
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interf
- Dialing and Number
- Electronic Switche
- Flexible Code Res
- Incoming Digit Tra
Managing: 10.10.10.131 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00
Distant Steering Code List
Add
Please enter a distant steering code 2
to Add
Managing: 10.10.10.131 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Coordinated Dialing Plan (CDP) » Distant Steering Code
Steering Code
Distant Steering Code
Distant Steering Code: 2
Flexible Length number of digits: 4 (0 - 10)
Display: Local Steering Code (LSC)
Remote Radio Paging Access:
Route List to be accessed for trunk steering code: 10
Collect Call Blocking:
Maximum 7 digit NPA code allowed:
Maximum 7 digit NXX code allowed:
Submit

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

247

Notes

_____

_____

_____

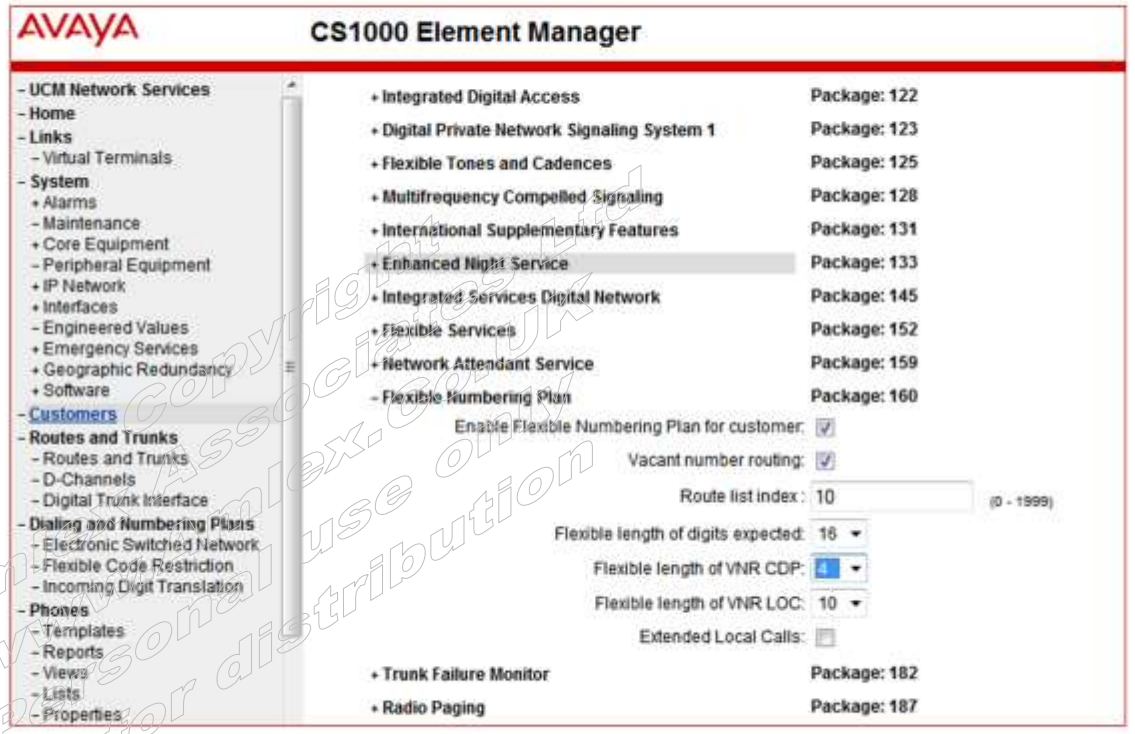
_____

Vacant Number Routing

The alternative to Distance steering codes is the use of Vacant Number Routing. This is a form of “Catch All” routing as it sends any number not configured on the system to a specified route, usually a Virtual Trunk route. Thus the routing of the request is passed from the Call server to the NRS for its ultimate destination.

Using VNR can reduce the routing table/steering codes on the Call server but it can lead to misdirected calls if careful attention isn’t paid to the routes needed.

To configure VNR in the Element Manager select **CUSTOMER / 00 / FEATURE PACKAGES / PACKAGE 160**. Remember to set the number of digits expected to the correct length to avoid a long post dial delay.



Amlex Copyright Associates Ltd www.amlex.co.uk Personal use only Not for distribution

248

Notes

_____

_____

_____

_____

22. Network Routing Service - NRS

The Network Routing Service (NRS) is a separate software subsystem deployed onto a Linux server which deals with the routing of Virtual Trunk calls.

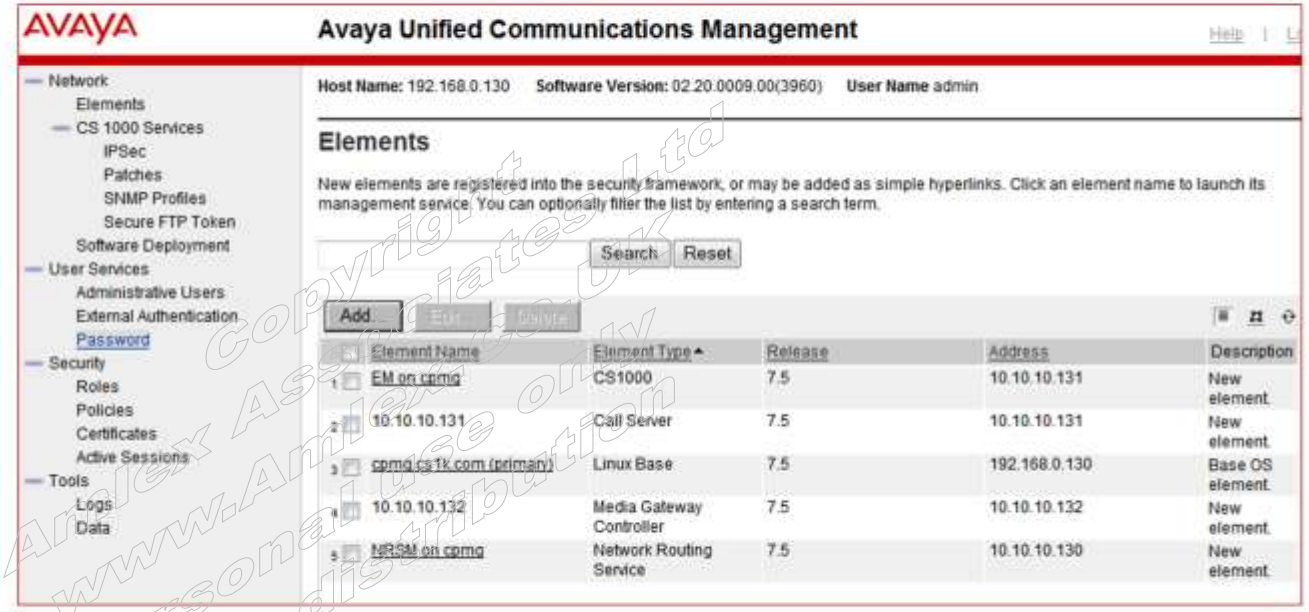
The NRS is effectively a SIP proxy & redirect serve, an H.323 Gatekeeper as well as a Network connect server for Unistim. The Network Connect Server has the job of redirecting IP sets in three specific scenarios.

- ❑Network Virtual Office
- ❑Geographic Redundancy
- ❑Branch Office

In essence the NCS redirects sets to the IP Node to register at for these applications.

NRS can be deployed on a CoRes Call server along with Subscriber Manager but not on a Primary UCM not supporting a Cores Call server but running Subscriber Manager.

It is accessed from the UCM Elements list as shown here and needs some configuration even before a backup of an NRS is loaded.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

249

Notes

_____

_____

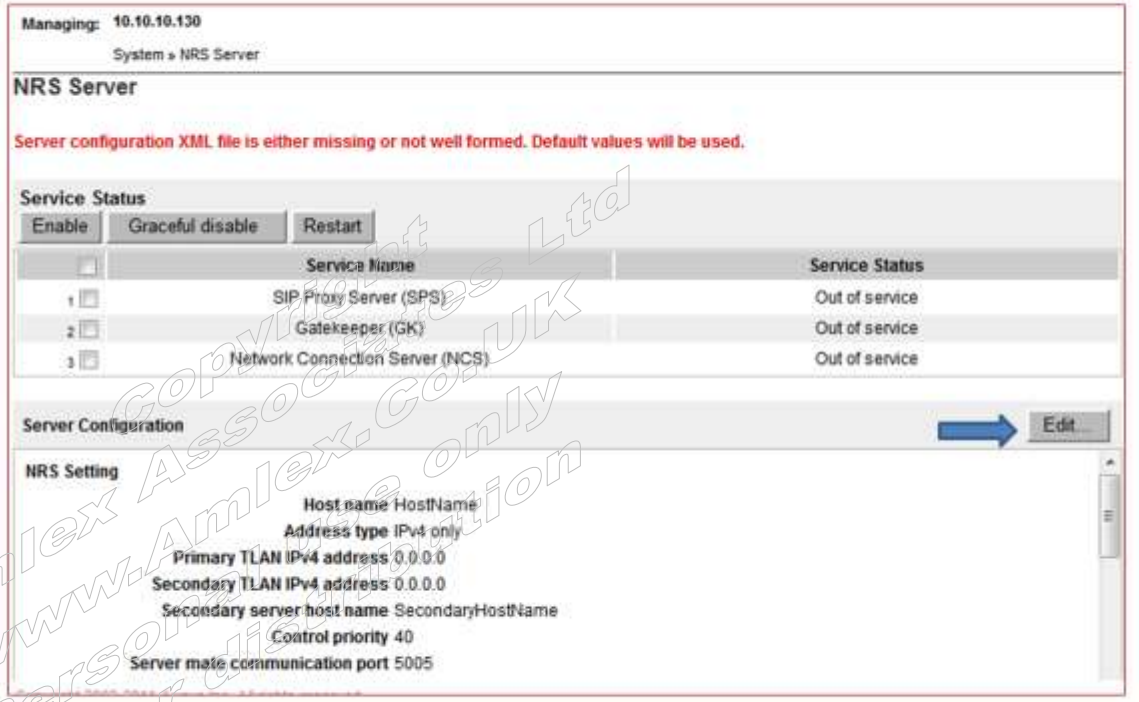
_____

_____

NRS Server Settings

As you can see from the example here, when the NRS is first deployed it will not run without some configuration.

To complete the initial setup and bring the components into service first click on the EDIT button as shown.


Managing: 10.10.10.130
System » NRS Server
NRS Server
Server configuration XML file is either missing or not well formed. Default values will be used.
Service Status
Enable
Graceful disable
Restart
Service Name
Service Status
1 SIP Proxy Server (SPS) Out of service
2 Gatekeeper (GK) Out of service
3 Network Connection Server (NCS) Out of service
Server Configeration
Edit
NRS Setting
Host name HostName
Address type IPv4 only
Primary TLAN IPv4 address 0.0.0.0
Secondary TLAN IPv4 address 0.0.0.0
Secondary server host name SecondaryHostName
Control priority 40
Server mate communication port 5005

Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

250

Notes

_____

_____

_____

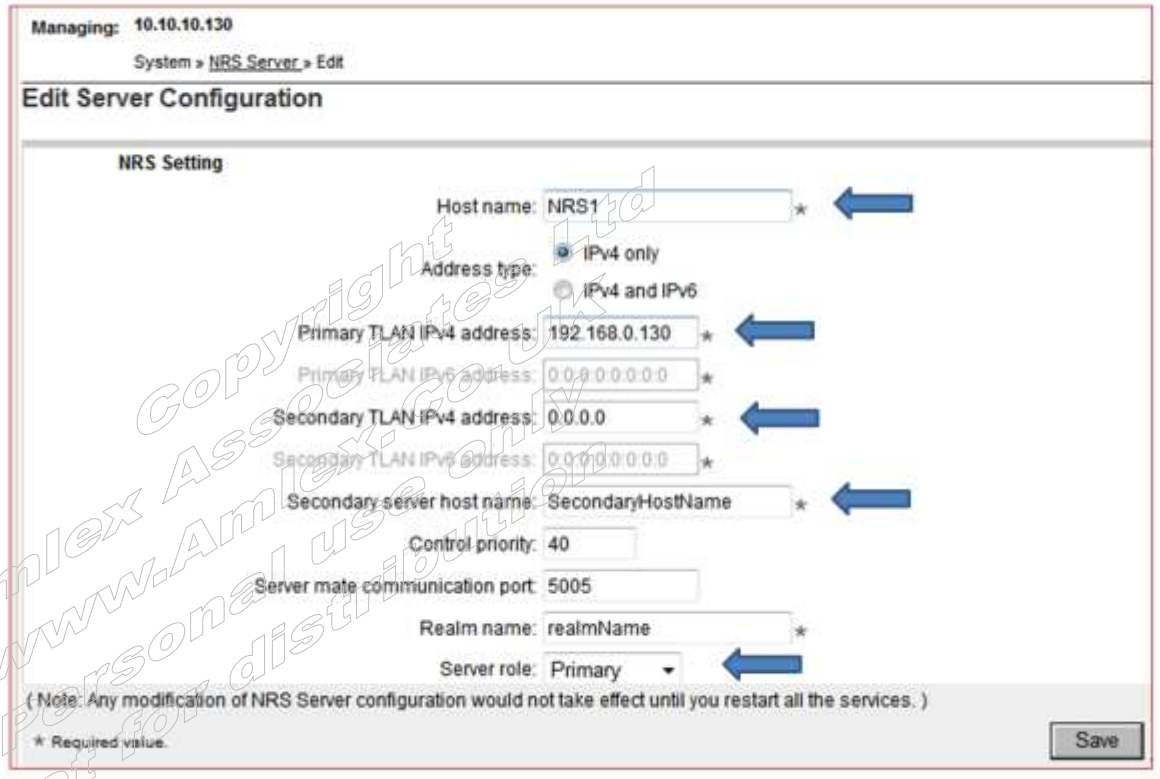
_____

Global Settings

When editing these global settings you first need to add the TLAN address and Name of the Primary NRS and the same for the secondary if there is one.

Make sure you choose the correct **SERVER ROLE , PRIMARY / SECONDARY** for the system you are editing.

In release 6 & 7 the Primary and Secondary synchronise immediately there is a change in the database, and the Endpoints are registered to both simultaneously.


Managing: 10.10.10.130
System » NRS Server » Edit
Edit Server Configuration
NRS Setting
Host name: NRS1
Address type: IPv4 only
IPv4 and IPv6
Primary TLAN IPv4 address: 192.168.0.130
Primary TLAN IPv6 address: 0:0:0:0:0:0:0:0
Secondary TLAN IPv4 address: 0.0.0.0
Secondary TLAN IPv6 address: 0:0:0:0:0:0:0:0
Secondary server host name: SecondaryHostName
Control priority: 40
Server mate communication port: 5005
Realm name: realmName
Server role: Primary
(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)
* Required value.
Save

251

Notes

_____

_____

_____

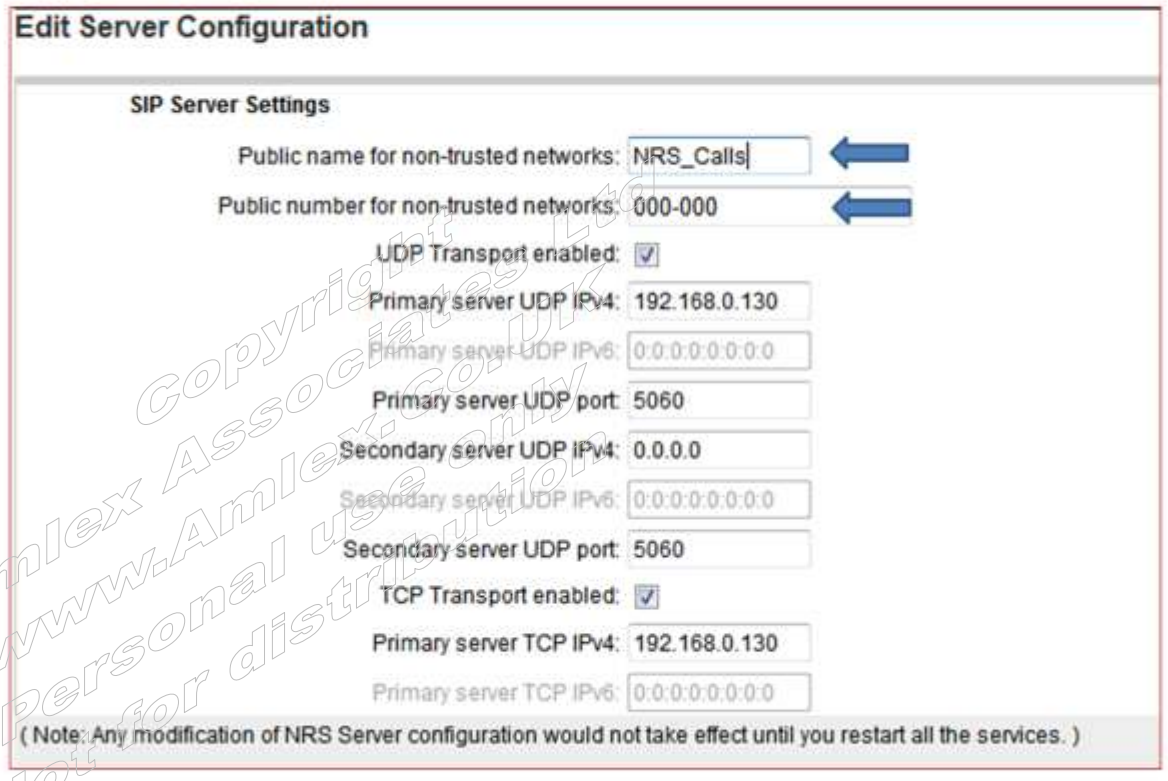
_____

Copyright Amlex Associates Ltd

SIP Settings

Scrolling down from the NRS settings you will find the SIP settings were you define which Protocols you wish to support. Ensure you tick all that apply.

Again you need to add the IP addresses as required.


Edit Server Configuration
SIP Server Settings
Public name for non-trusted networks: NRS_Calls
Public number for non-trusted networks: 000-000
UDP Transport enabled:
Primary server UDP IPv4: 192.168.0.130
Primary server UDP IPv6: 0:0:0:0:0:0:0:0
Primary server UDP port: 5060
Secondary server UDP IPv4: 0.0.0.0
Secondary server UDP IPv6: 0:0:0:0:0:0:0:0
Secondary server UDP port: 5060
TCP Transport enabled:
Primary server TCP IPv4: 192.168.0.130
Primary server TCP IPv6: 0:0:0:0:0:0:0:0
(Note: Any modification of NRS Server configuration would not take effect until you restart all the services.)

252

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

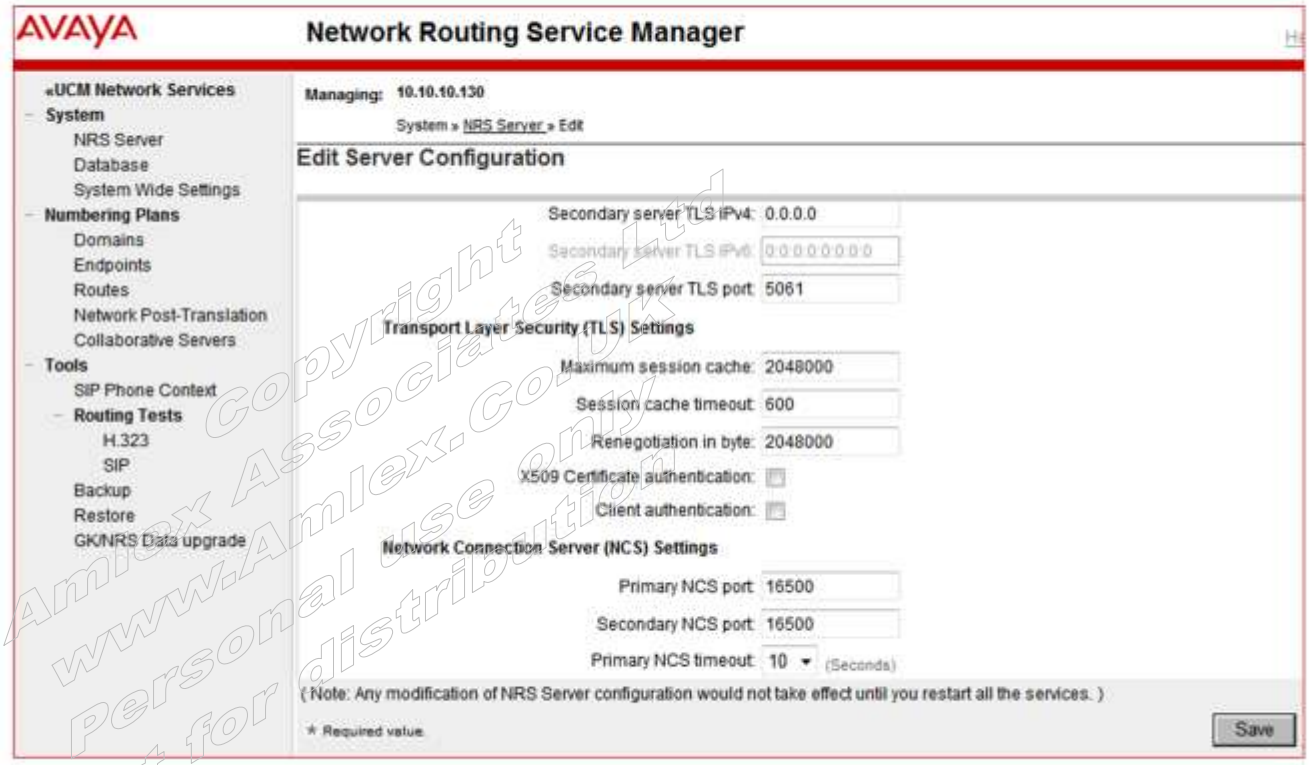
_____

TLS

Even further down you will find the TLS settings for SIP and NCS settings. TLS Transport Layer Security is a way of encrypting SIP messages and is suited to external SIP connections.

Generally the default values for Timeouts and Port numbers will be fine and should only be changed when necessary.

When you have configured all these **SAVE** the settings before starting the services.



Amlex Associates Ltd Copyright www.Amlex.Co.Uk Personal use only Not for distribution

253

Notes

_____

_____

_____

_____

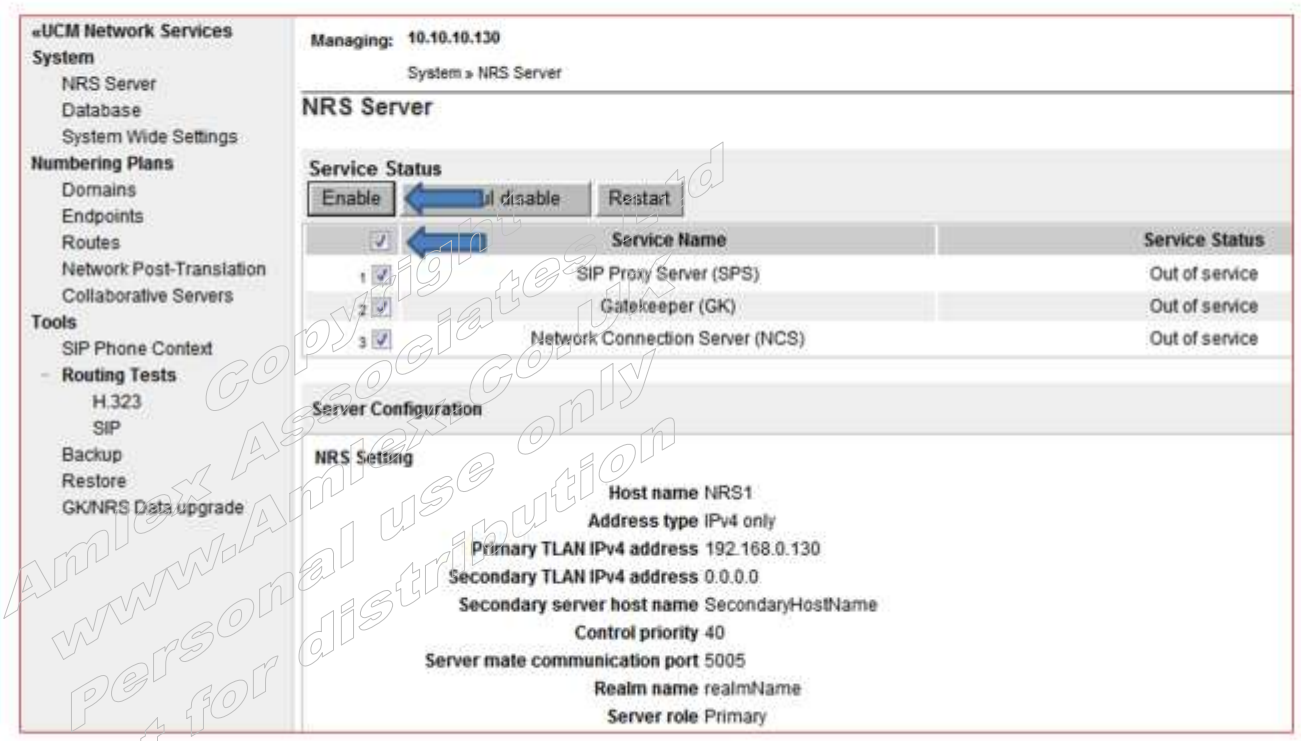
Enable/Restart Services

Once the System settings are completed it is time to start the three services.

Tick the boxes for all three SPS, GK and NCS and click the **ENABLE** button.

It may take a minute or so for the services to start so refresh the screen until you get the ”IN SERVICE” rather than “ÖUT OF SERVICE””message.

If one of the components refuses to start try clicking the **RESTART** button once with it selected by the tick box.



Amlex Associates Ltd Copyright
www.Amlex.co.uk
Personal use only
Not for distribution

254

Notes

_____

_____

_____

_____

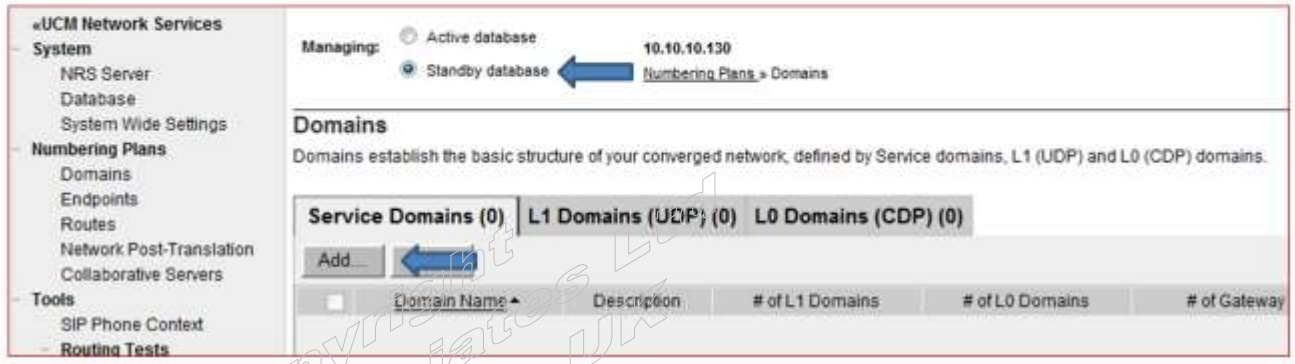
Copyright Amlex Associates Ltd

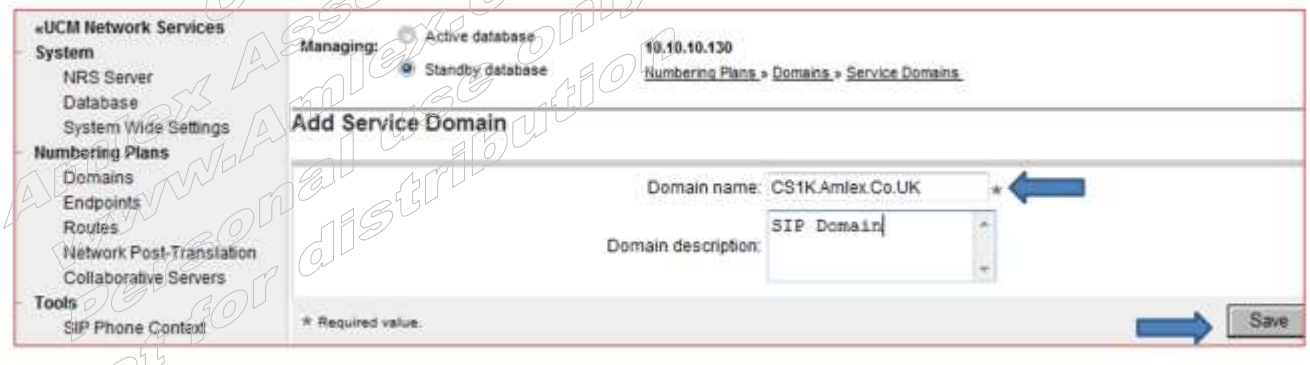
Add the Service Domain

The NRS database is built as an Active / Standby application. To add or edit configuration details you need to be in the **STANDBY DATABASE** as shown using the radio button at the top of the screen.

Once configuration is completed you can then place the Standby database into Active mode to use and test it. Changes do not take effect till they have been committed.

The first thing to add is the Domains, starting with the Service Domain. Select **NUMBERING PLANS / DOMAINS** and click on the ADD button for Service Domains. Enter the Domain name and a description and SAVE using the button shown.





Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

255

Notes

_____

_____

_____

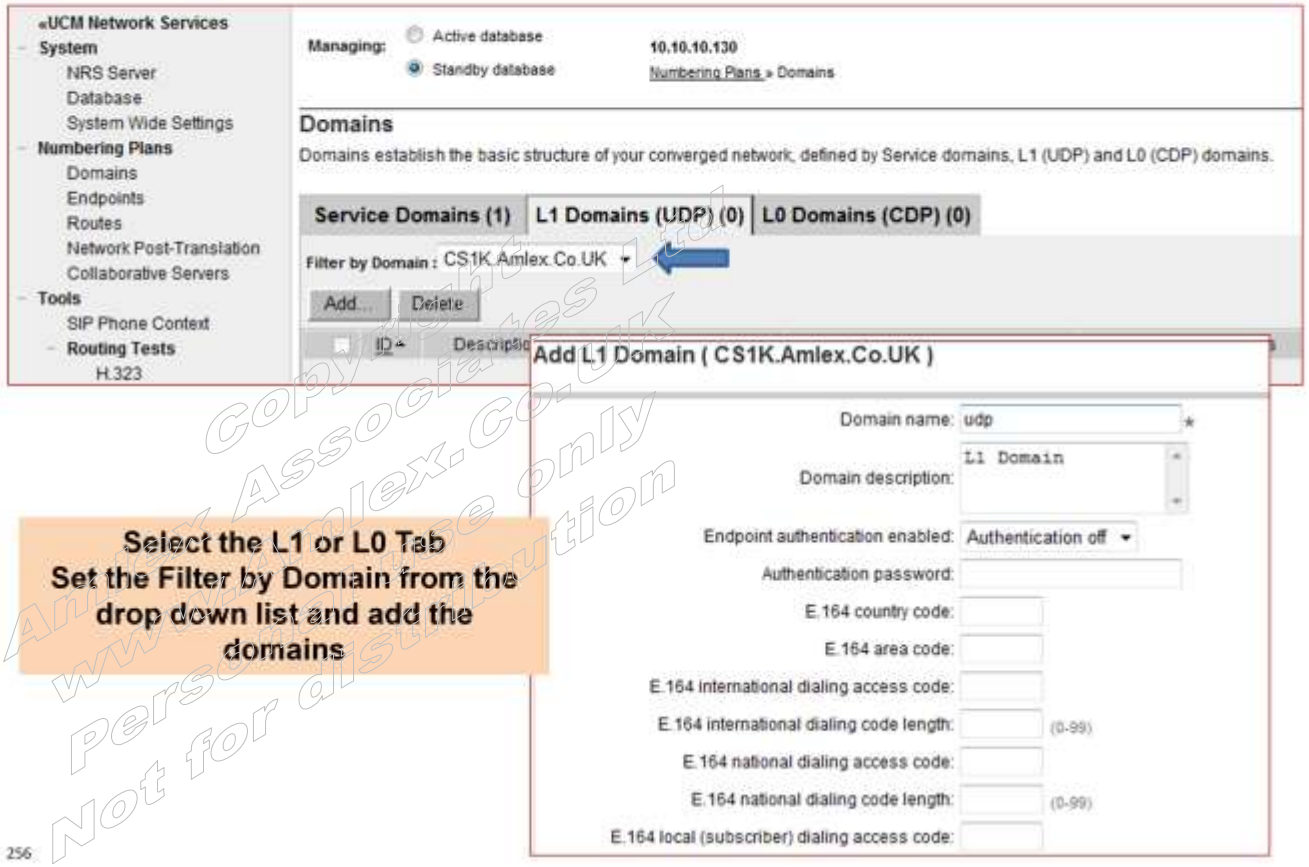
_____

Add L1 – UDP & L0 – CDP Domains

Next we need to add the L1 and L0 Domains which equate to the UDP and CDP dial plans of the Call Server.

Select the LI DOMAINS (UDP) tab as shown, select the correct Service domain from the dropdown list and add the UDP domain using th defaults for our example.

Repeat the process for the L0 CDP Domain.



Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

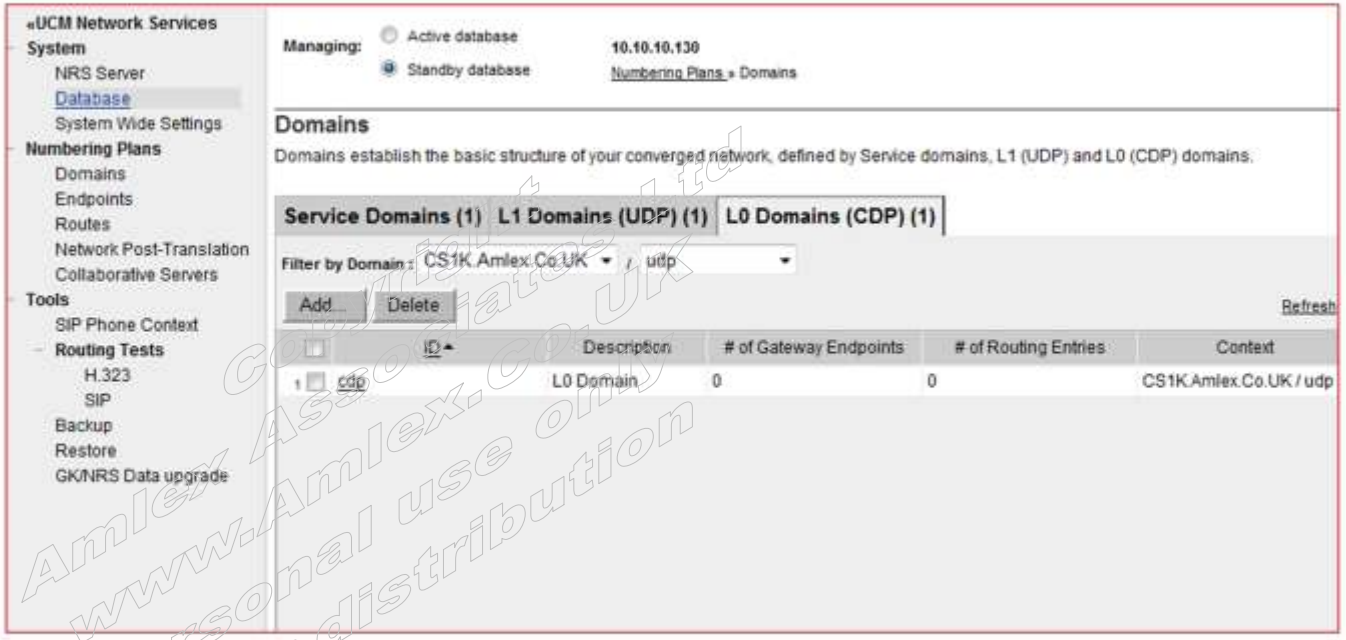
_____

_____

_____

SIP URI Domains

When completed you will have something like the display shown. We have used the defaults UDP and CDP for L1 and L0 but in a customer situation these should map to their own domain structure.



257

Notes

_____

_____

_____

_____

Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

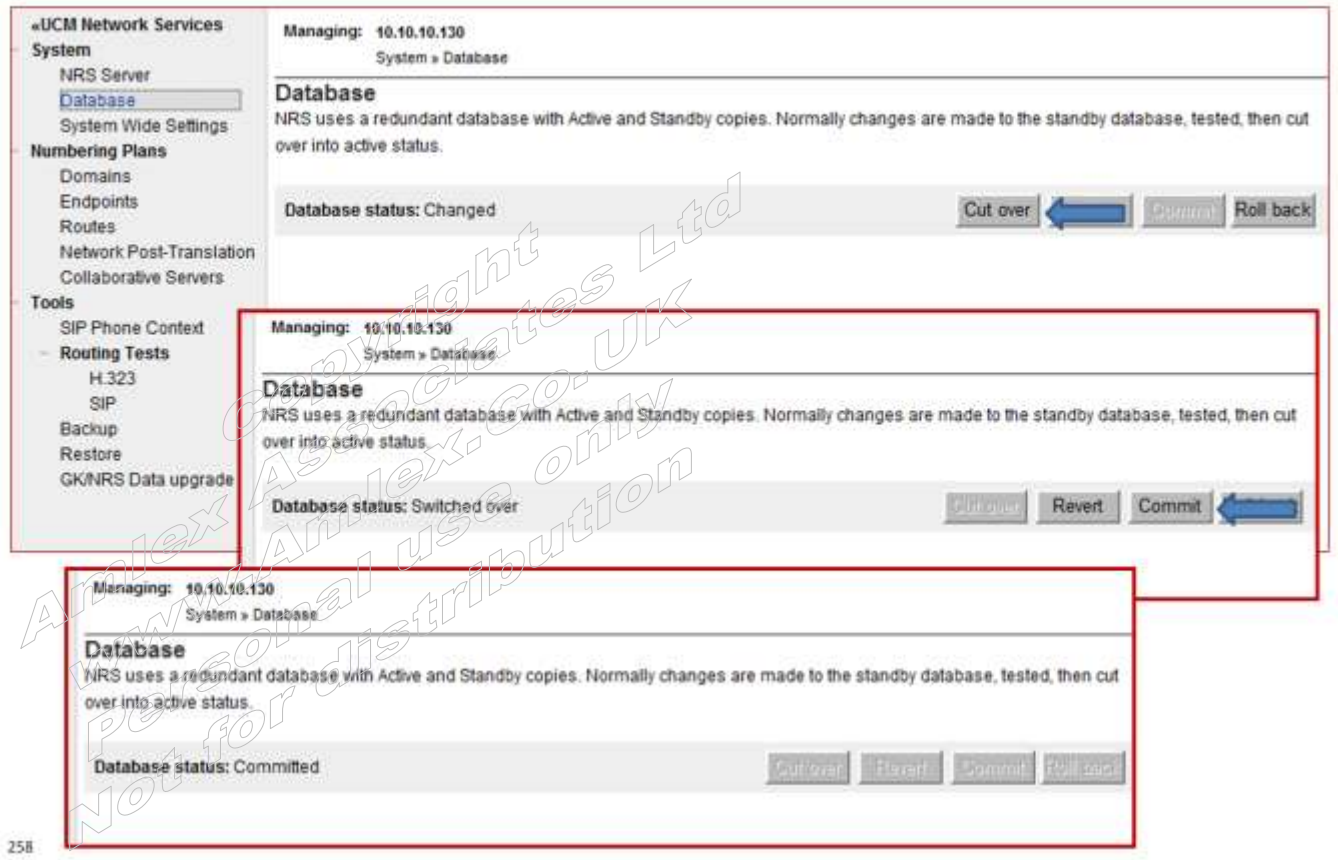
Saving Database

Once you have configuration data that you wish to save and put into service, select the **SYSTEM / DATABASE** option from the menu.

The screen as shown will display a message that the database status is changed and offer you the buttons to **CUT OVER** from the Standby to the Active mode.

As you will see in the second picture after the cut over the buttons then change to allow you to Revert (back to Previous settings) or Commit.

If you are happy with the changes after testing then you simply click on the **COMMIT** button to make the changes permanent.



Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

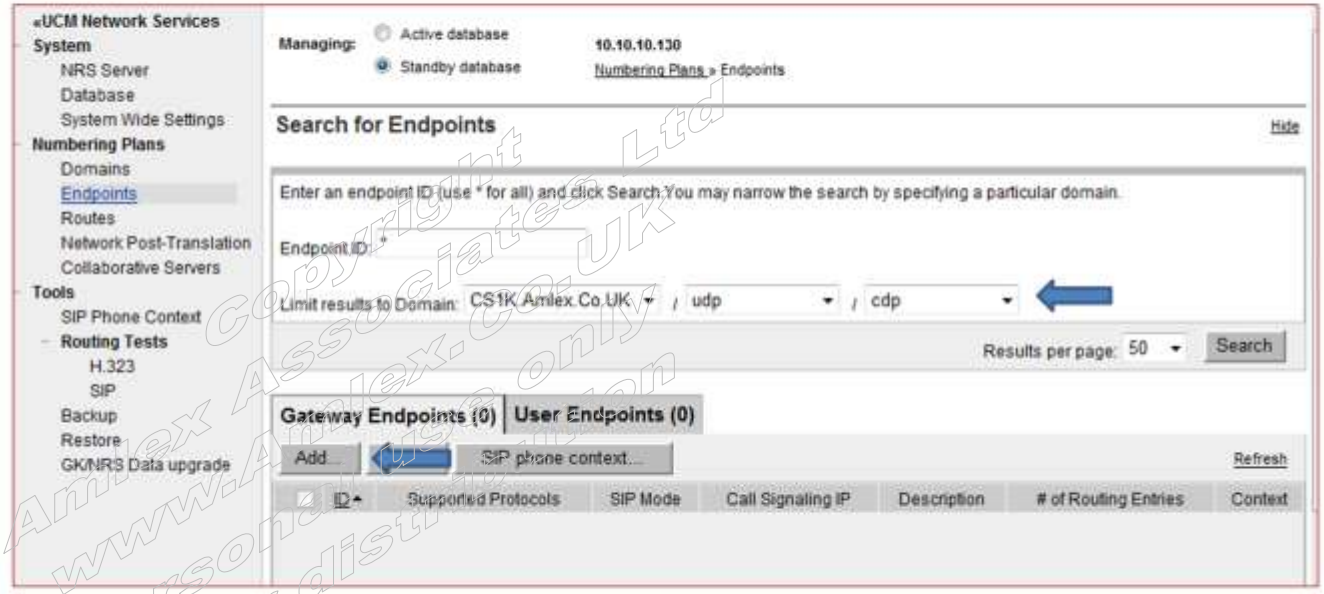
_____

Add Endpoints

Once you have the basic Domain structure in place you can then add the system endpoints in the relevant domains. Be sure you select the Gateway Endpoints tab when adding a signalling gateway not a User Endpoint.

Select the option **NUMBERING PLANS / ENDPOINTS**, ensure you are back in the Standby database and set the Domain you want to add the endpoints to ("Limit Results to Domain " drop down menus).

Clicking the **ADD** button will take you to the configuration screen



Copyright Amlex Associates Ltd
www.Amlex.co.UK
Personal use only
Not for distribution

259

Notes

_____

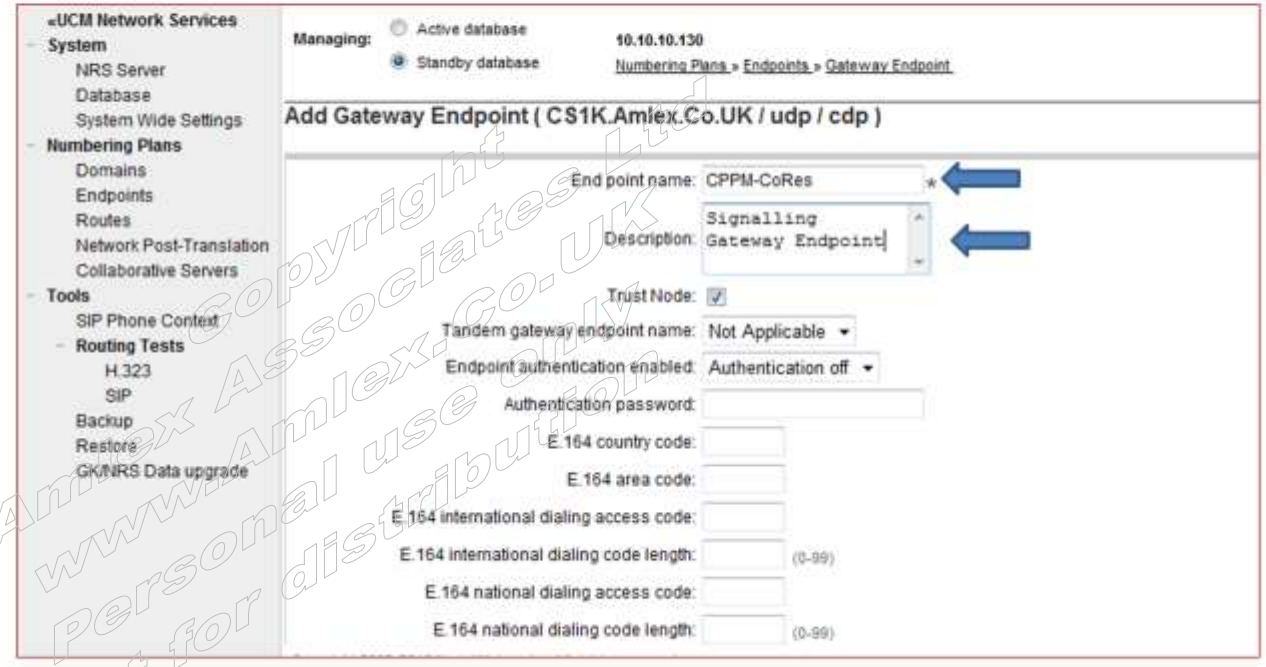
_____

_____

_____

Endpoint Name

The example shows the Endpoint being added. It essential that the End Point Name matched exactly the name entered into the IP node of the Signalling gateway. If this is different the Endpoint will not register and no exchanges will occur, effectively shutting down any Virtual Trunk traffic.



Amlex Associates Ltd ©Copyright www.Amlex.Co.UK Personal use only Not for distribution

260

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

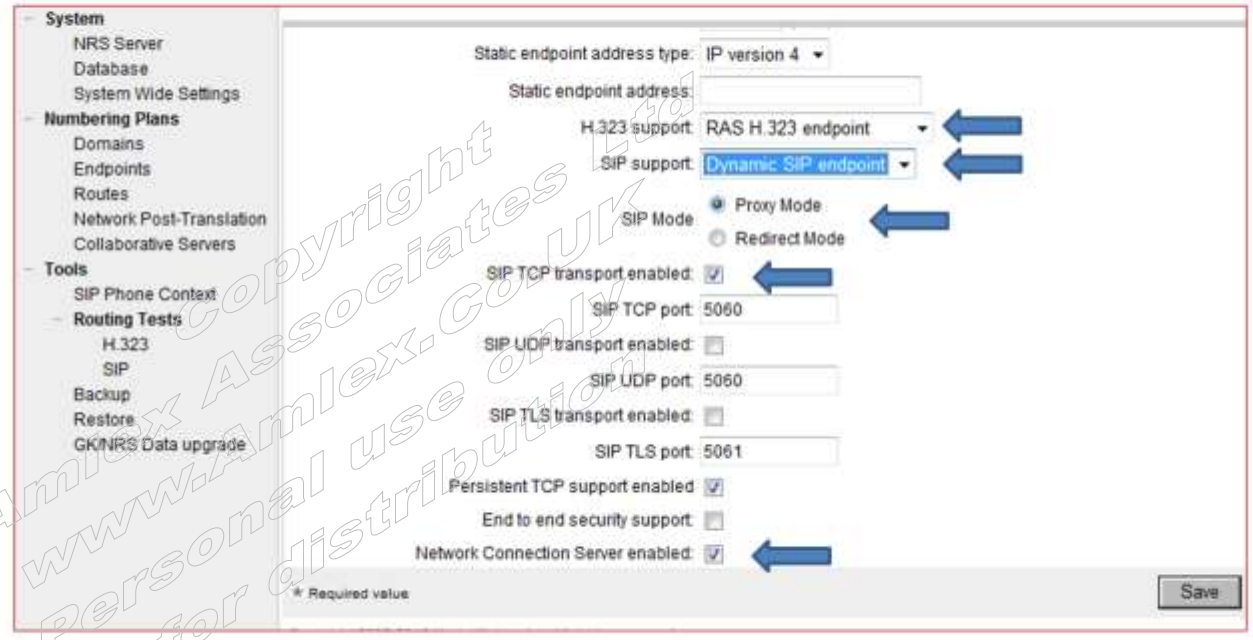
Define Protocols to Use

Scroll down to set the Protocols to be used by the endpoint. Here we are using both SIP & H323.

The option selected here is for RAS H323 and Dynamic SIP this means that they will find the Gateways without entering the Static IP address. This is probably the best option for configuration but if necessary a static address can be used.

Notice also that this is where you select whether to have a SIP redirect function or full SIP Proxy. In addition you need to select which protocol SIP will use for its messages. Nortel recommends TCP as shown here but you may want to use TLS to add security.

Finally note that the box for the Network Connection Server has been ticked to enable this service also. NCS is used for Network Virtual Office, Branch Office and Geographic Redundancy.



Amlex Copyright
www.Amlex.Co.UK
Personal use only
Not for distribution

261

Notes

_____

_____

_____

_____

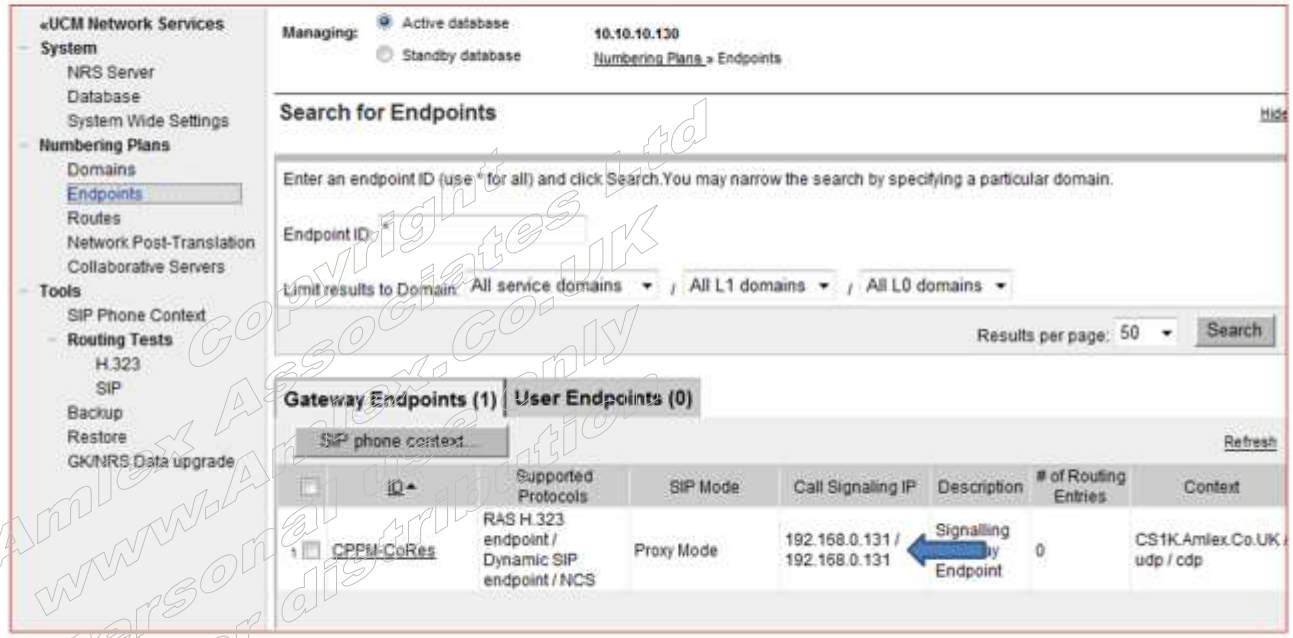
Copyright Amlex Associates Ltd

Registered Endpoint

Once you have added the endpoints required you again need to Cut Over the database to the Active Mode.

Once you view the End Points in the Active database you will see that the Node IP address is displayed under the CALL SIGNALLING IP column.

This shows that the gateway has registered and is always the first thing to check when there are problems with Virtual Trunks.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

262

Notes

_____

_____

_____

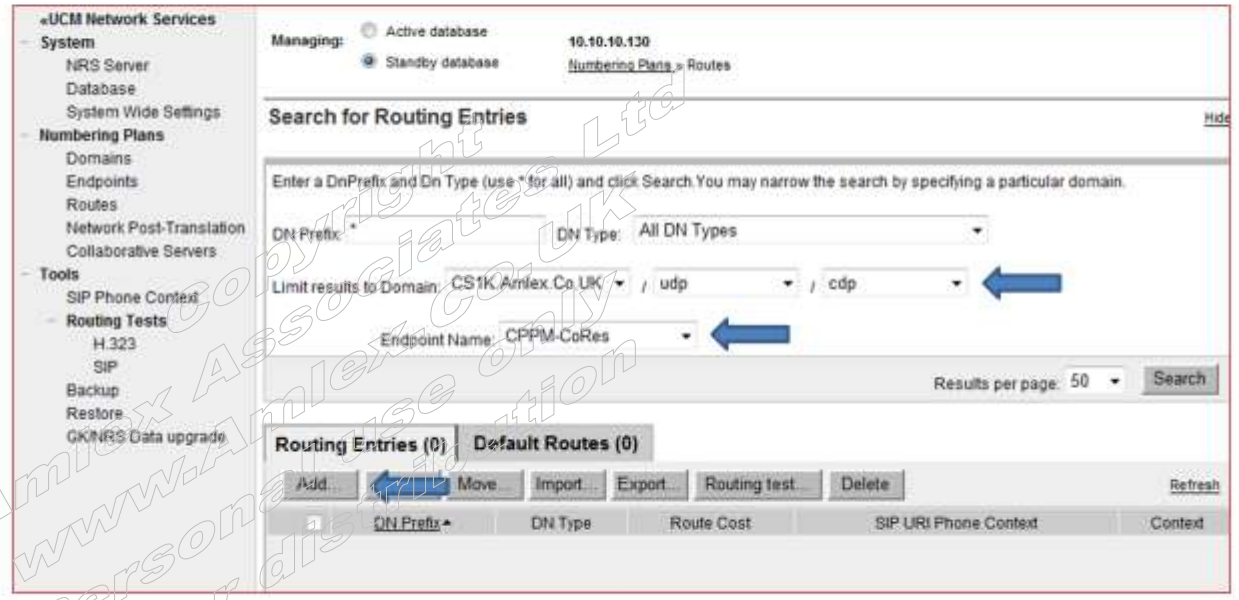
_____

Route Entry

Finally we can now add the Routing entries to the endpoints. Select the option **NUMBERING PLANS / ROUTES** in the standby database and navigate to the correct Domains and endpoint.

Using the **ROUTING ENTRIES** tab **ADD** the entries required for the particular endpoint.

For the NRS, route information is added for DN's which you want directed to the Endpoint to be terminated. i.e. If the endpoint has the extension range 1xxx we add a route for DN's starting with a 1 to the endpoint.



263

Notes

_____

_____

_____

_____

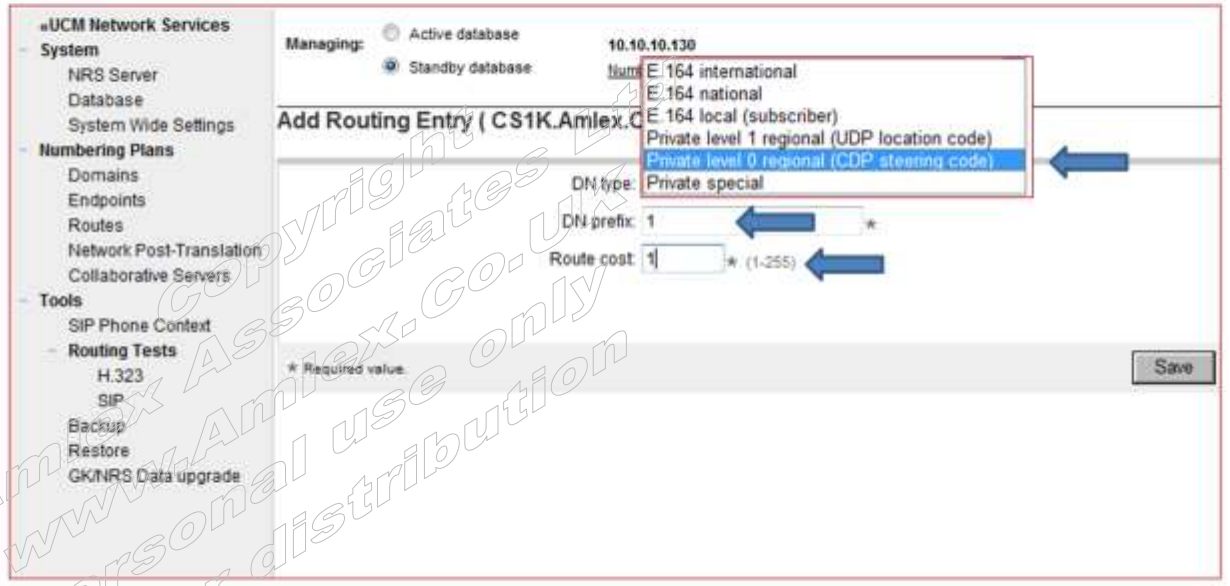
Copyright Amlex Associates Ltd

Call Type

One of the most important things is to get the correct Call Type when adding the route.

For a simple CDP extension dialling scheme all we need is a CDP call type along with the DN prefix in this case 1 and then a route cost again 1 here.

The Route Cost is used to give priority to one route over another when there are multiple options.



Amlex Associates Ltd
www.Amlex.Co.uk
Personal use only
Not for distribution
Copyright

264

Notes

_____

_____

_____

_____

AVAYA
Communications Server 1000
Release 7.5

Part 3

Installation, Configuration,
Support & Troubleshooting

Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

265

Copyright Amlex Associates Ltd

With Release 7.5 comes the integration into the Avaya Aura Architecture allowing the CS1K to become a part of the Aura environment and interconnect with Communications Manager.

The System Manager becomes the new Primary UCM for the CS1K and also is necessary to manage the Session Manager.

The Session Manager takes on the role of the NRS for SIP call Routing and also that of the NCS for set redirection for Branch office Geographic redundancy and Virtual office.

23. Avaya Aura Migration

- Avaya Aura System for CS1K Migration
  - System Manager
    - Runs the UCM for CS1K and Session Manager
  - Session Manager
    - Replaces NRS for SIP Routing and NCS function
      - No H.323 support
- Migration for SIP based Networks
  - Exceptions
    - Using H.323
    - High Scalability systems
    - IP Version 6

266

Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

Notes

_____

_____

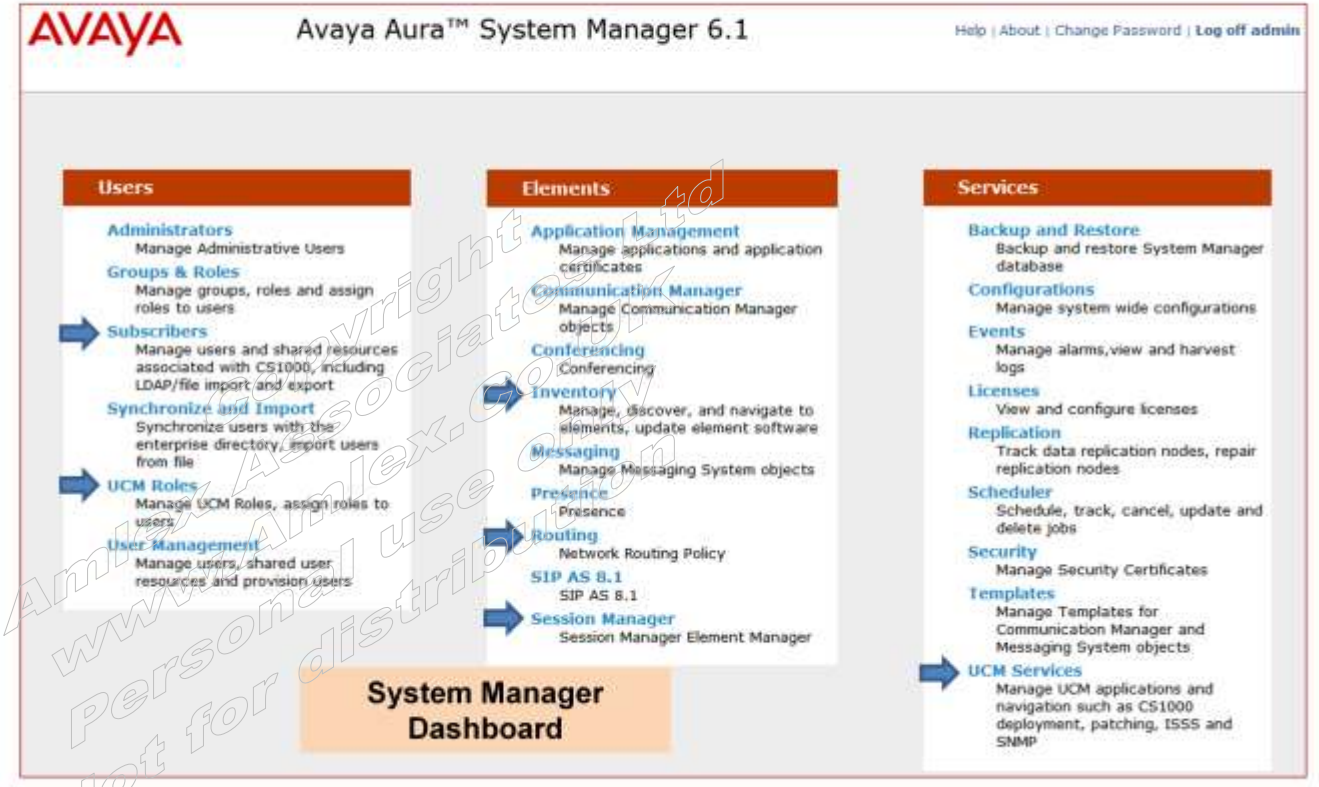
_____

_____

Aura System Manager Dashboard

When integrated to the Aura environment you will login to the System Manager and be presented with the "Dashboard" view as shown here.

The Arrows highlight the main areas used in a CS1K implementation.



Amlex Associates Ltd
www.Amlex.com
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

To migrate from the Release 6 CS1K model to the Aura environment the major steps are shown.

The first option is to move call routing off the NRS to the Session Manager by converting the NRS database and importing it into Session manager. In addition new TPS instances are created to replicate the NCS functionality.

Once call routing is switched over the UCM can be enabled in the System Manager and then the existing CS1K servers reregistered to it as the new Primary UCM.

With this done it is simply a case of adding the software to the Deployment Manager and upgrading the servers.

This example assumes the System and Session Managers are both currently installed.

Migration from CS1K Rel 6 to Aura

- Migrate NRS data to Session Manager
  - Convert NRS Db
  - Import to Session Manager
  - Create NCS entities & Routing
  - Rel 6 Systems will be able to work correctly with Session manager rather than NRS.
- Turn on UCM within System Manager
- Register Rel 6 servers to System Manager as Primary UCM
  - Base Manager Security Config
- Upload Software to System Manager/UCM Deployment Manager
  - NOTE:- as Linux may also be installed at Rel 7 a Linux .iso file may be required.
- Configure Pre-Deployment of re-registered servers
  - Configure Applications to run
  - If New Servers are used (i.e. Changing H/W) configure as new deployments – e.g. Linux Base & Applications.
  - Run Upgrades or Installations as appropriate
  - NFS Installation is available from the System manager

268

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for commercial use without authority

Notes

_____

_____

_____

_____

To migrate the NRS it must first be converted to only Static endpoints.

The database is then saved and the nrs.xml file converted using the online tool. This creates all of the necessary fields for the session manager and resolves the issue of the CDP>UDP context used by Nortel.

NRS to Session Manager 1

- Migrate NRS data to Session Manager
  - Install SPS Patch
    - Converts NRS database to Static Endpoints
    - Save converted NRS Database & extract nrx.xml file
- Access online conversion tool
  - Make sure you have Session Manager information
    - Management and SIP address
  - Access tool at https://nrstool.avaya.com/default.aspx
  - Login to convert database
  - Edit SIP entities to match Session manager
  - Add Adaption information
    - Required to resolve issues with "CDP.UDP" Context
  - Download file ready to Import to Session Manager

269

Copyright Amlex Associates Ltd www.amlex.com Personal use only Not for distribution

Notes

_____

_____

_____

_____

On the Session manager we need to check it is running correctly and then import the converted file which will bring over the NRS routes.

We then add the TPS instances for the NCS and the routing information associated.

Finally the IP nodes on the CS1K systems are edited to point to the Session Manager for both SIP and NCS.

NRS to Session Manager 2

- Login to System Manager and access Session Manager
  - Check system is up and running correctly
  - Import "sm_data_client.zip" from conversion tool.
  - Check import and that Session manager is monitoring Endpoints.
- Create TPS entities in System Manager inventory
  - Replaces NCS endpoints
  - Add NRS Proxy Users in Session Manager (NCS Routes)
- In Element Manager for all CS1K Nodes
  - Edit IP Telephony Node
  - Point SIP requests to Session Manager (SIP address)
  - Point NCS requests to Session Manager (SIP address)
- IP sets should correctly redirect and SIP calls be routed correctly

Copyright Amlex Associates Ltd www.Amlex.co.UK Personal use only Not for distribution

270

Notes

_____

_____

_____

_____

The SPS patch must be installed via the CLI to the NRS server. This can be done using SFTP to copy it to the right directory and then issuing the Linux commands

pload to load the patch and generate a patch Handle, then :-

pins to bring the patch into service.

With the patch in service and the endpoints correctly registered run the command to convert SIP endpoints :-

spsDynamic2Static

Once completed reopen the NRS to check all endpoints are now static.

If you are converting a Rel 7.5 NRS to the Session Manager there is no patch available so you need to login to the NRS and convert each SIP endpoint manually to static, adding the IP Node address.

Finally backup the NRS database and download it to a PC and extract the file nrs.xml which is used with the online conversion tool.

Install SPS Patch

- The SPS patch must be selected to match the current release. Install the patch using the CLI only onto the NRS server
  - Copy to /var/opt/nortel/patch (SFTP)
  - Use **pload** and **pins** to install patch
    - nortel-cs1000-sps-6.00.18.65-09.i386.001.ntl – Rel 6
    - nortel-cs1000-sps-7.00.20.10-2.i386.000.ntl – Rel 7
- Ensure all endpoints are registered to the NRS then
  - Run the CLI command **spsDynamic2Static**
    - This will convert all the SIP endpoints from Dynamic to Static using the currently registered Node IP address
    - Database is committed during this process
- If Converting Rel 7.5 to Session Mgr - NO PATCH AVAILABLE
  - Manually convert SIP endpoints to Static and add Node IP Address
- Backup NRS and download file to PC
  - Extract nrs.xml from nrsback.tar ready for import to conversion tool

271

Copyright Amlex Associates Ltd www.amlex.com Personal use only Not for distribution

Notes

_____

_____

_____

_____

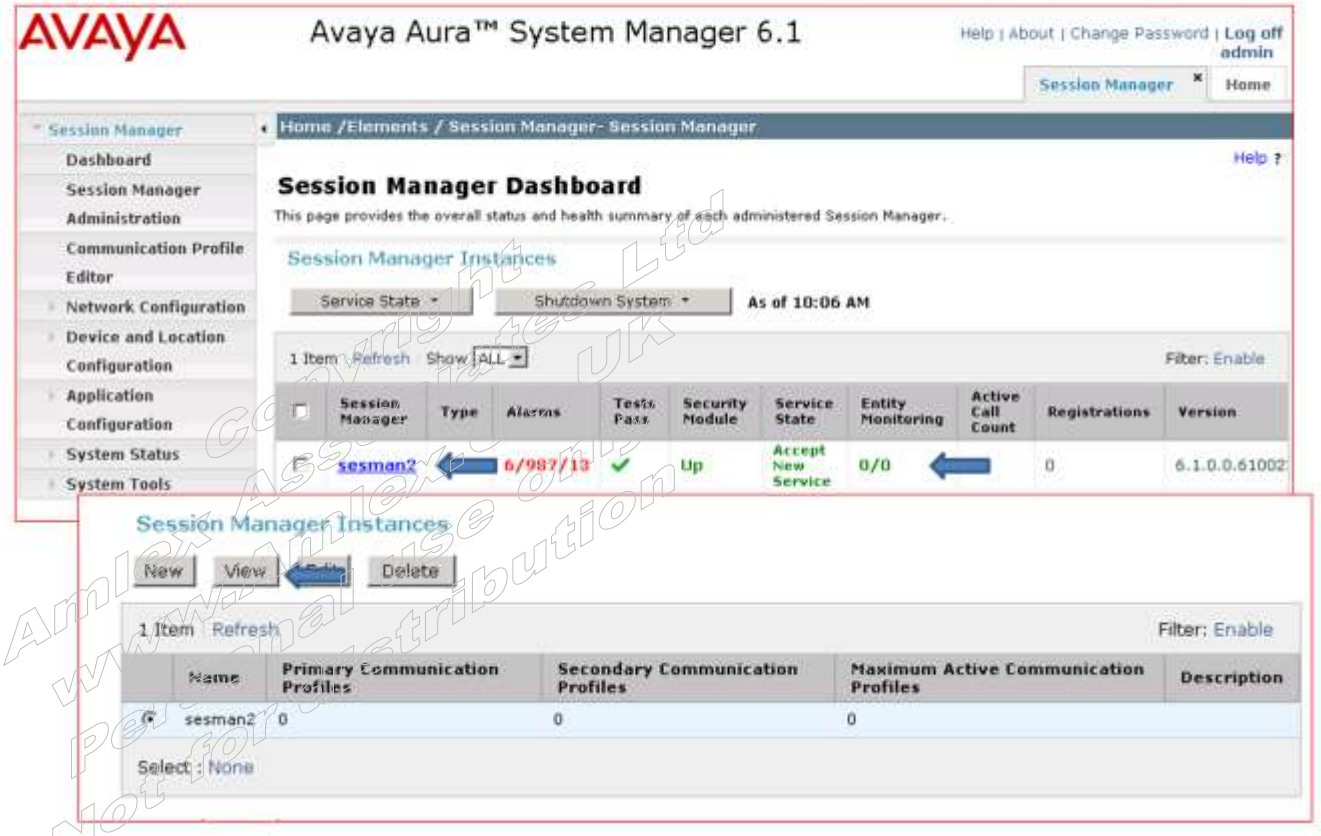
Check Session Manager Address

Before opening the online conversion tool login to the Session Manager and check that it is up and running correctly.

Note the green displays and particularly the Entity Monitoring 0/0. As this is a blank system there are no entities (endpoints) to monitor currently.

Click on the Link to the session Manager arrowed (sesman2) which will show the lower screen. To see the detail select the radio button and click the VIEW button.

See next slide



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

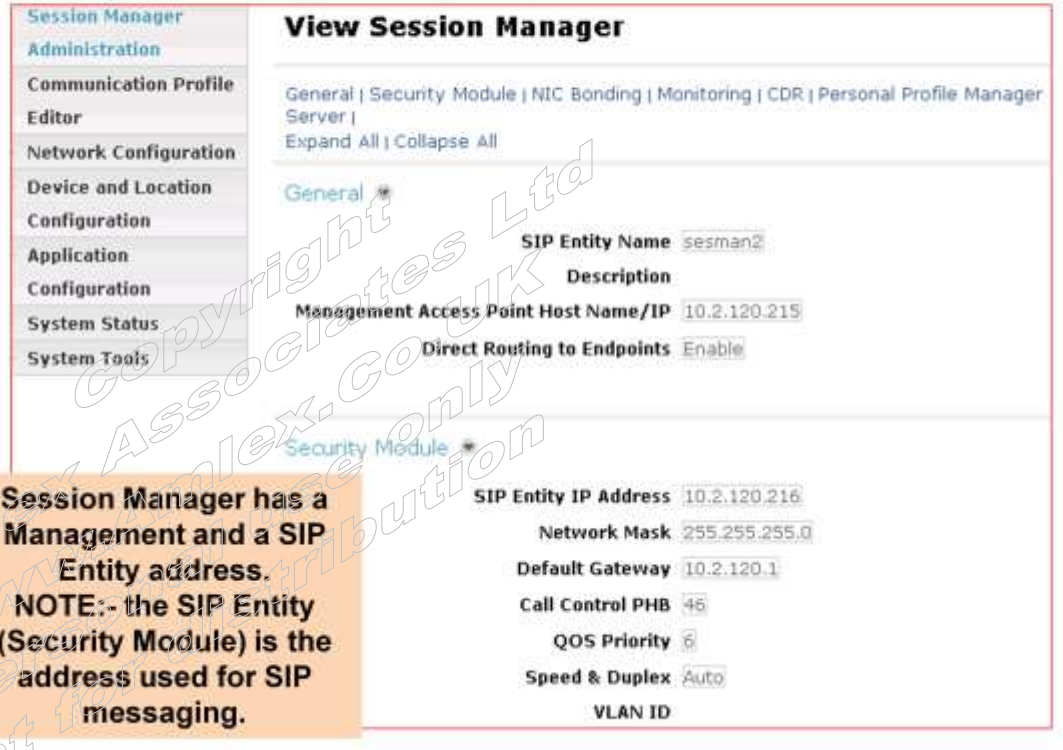
Session Manager Addresses

Here is the detail of the Session Manager.

As you can see it has two IP addresses and it is important to know the difference between them.

The management address is used for connecting to the system using Putty but for SIP signalling we use the SIP Entity Address (10.2.120.216 - here) .

You will need the SIP Entity IP address when converting the NRS so make a note of it.


Session Manager
Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
View Session Manager
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager Server |
Expand All | Collapse All
General
SIP Entity Name sesman2
Description
Management Access Point Host Name/IP 10.2.120.215
Direct Routing to Endpoints Enable
Security Module
SIP Entity IP Address 10.2.120.216
Network Mask 255.255.255.0
Default Gateway 10.2.120.1
Call Control PHB 46
QOS Priority 6
Speed & Duplex Auto
VLAN ID
Session Manager has a Management and a SIP Entity address.
NOTE:- the SIP Entity (Security Module) is the address used for SIP messaging.
273

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Convert NRS database

To convert the NRS login to the online tool and upload the nrs.xml file.

You will then be presented with the screen shown with the multiple Tabs.

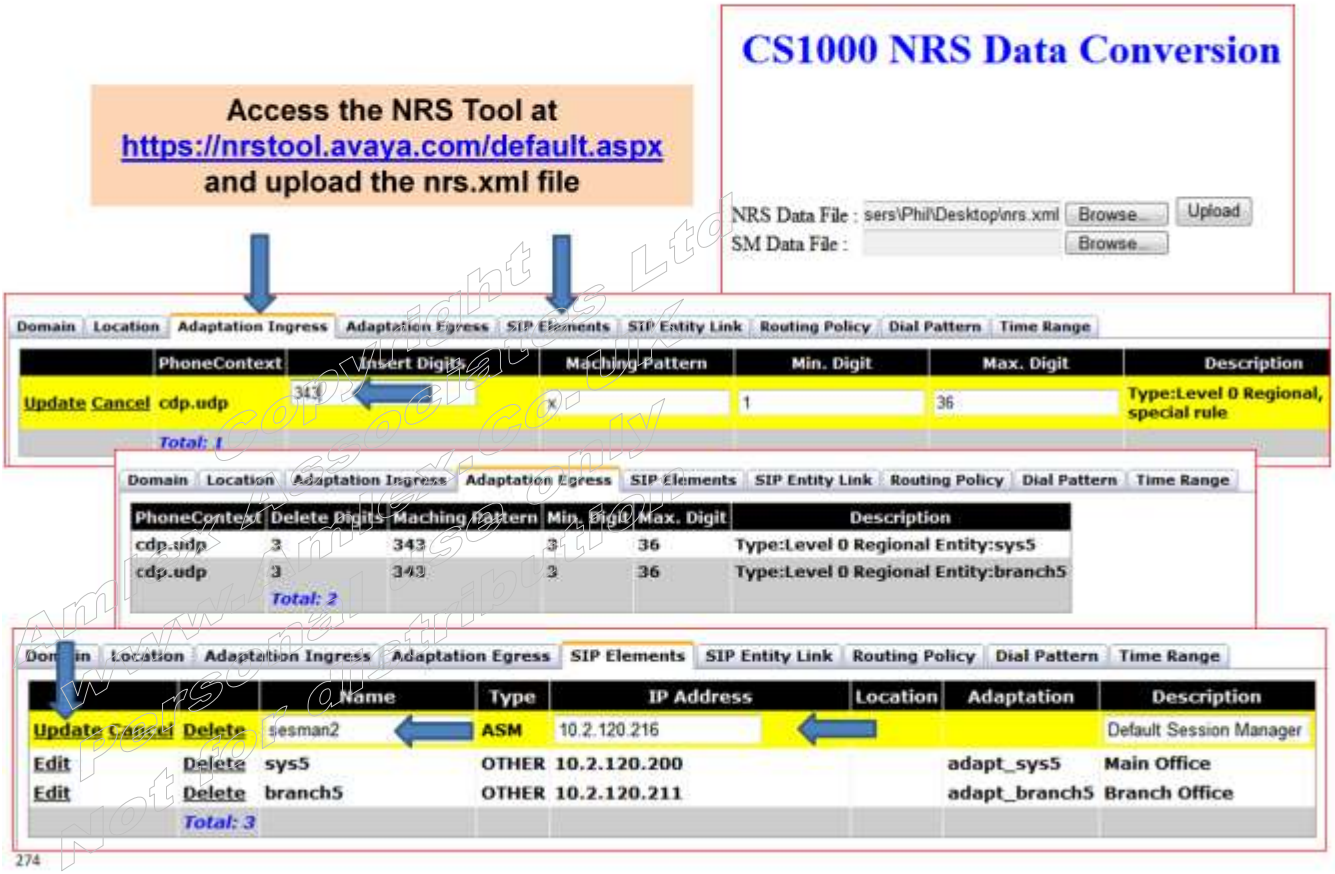
First select the Adaption Ingress tab and click edit. Here we are adding 343 as insert digits, this is because we cannot use the cdp.udp context that Nortel used in the past. The Insert digits (Usually the HLOC of the system) are inserted in front of the CDP extension digits and the cdp.udp context is deleted. Session manager can now route using this amended information.

The Adaption Egress is created automatically and does the reverse i.e. For calls back to a CS1K it removes 3 digits and adds back the cdp.udp context.

Finally we need to edit the SIP Elements to show the correct name of the Session manager and the SIP entity address.

Once the changes are made the file is downloaded from the tool ready to import into Session manager.

The filename is **sm_data_client.zip**.


Access the NRS Tool at
https://nrstool.avaya.com/default.aspx
and upload the nrs.xml file
CS1000 NRS Data Conversion
NRS Data File : sers\Phil\Desktop\nrs.xml
Browse...
Upload
SM Data File :
Browse...
Domain Location Adaptation Ingress Adaptation Egress SIP Elements SIP Entity Link Routing Policy Dial Pattern Time Range
PhoneContext Insert Digits Maching Pattern Min. Digit Max. Digit Description
Update Cancel cdp.udp 343 x 1 36 Type:Level 0 Regional, special rule
Total: 1
Domain Location Adaptation Ingress Adaptation Egress SIP Elements SIP Entity Link Routing Policy Dial Pattern Time Range
PhoneContext Delete Digits Maching Pattern Min. Digit Max. Digit Description
cdp.udp 3 343 3 36 Type:Level 0 Regional Entity:sys5
cdp.udp 3 343 3 36 Type:Level 0 Regional Entity:branch5
Total: 2
Domain Location Adaptation Ingress Adaptation Egress SIP Elements SIP Entity Link Routing Policy Dial Pattern Time Range
Name Type IP Address Location Adaptation Description
Update Cancel Delete sesman2 ASM 10.2.120.216 Default Session Manager
Edit Delete sys5 OTHER 10.2.120.200 adapt_sys5 Main Office
Edit Delete branch5 OTHER 10.2.120.211 adapt_branch5 Branch Office
Total: 3
274

Notes

_____

_____

_____

_____

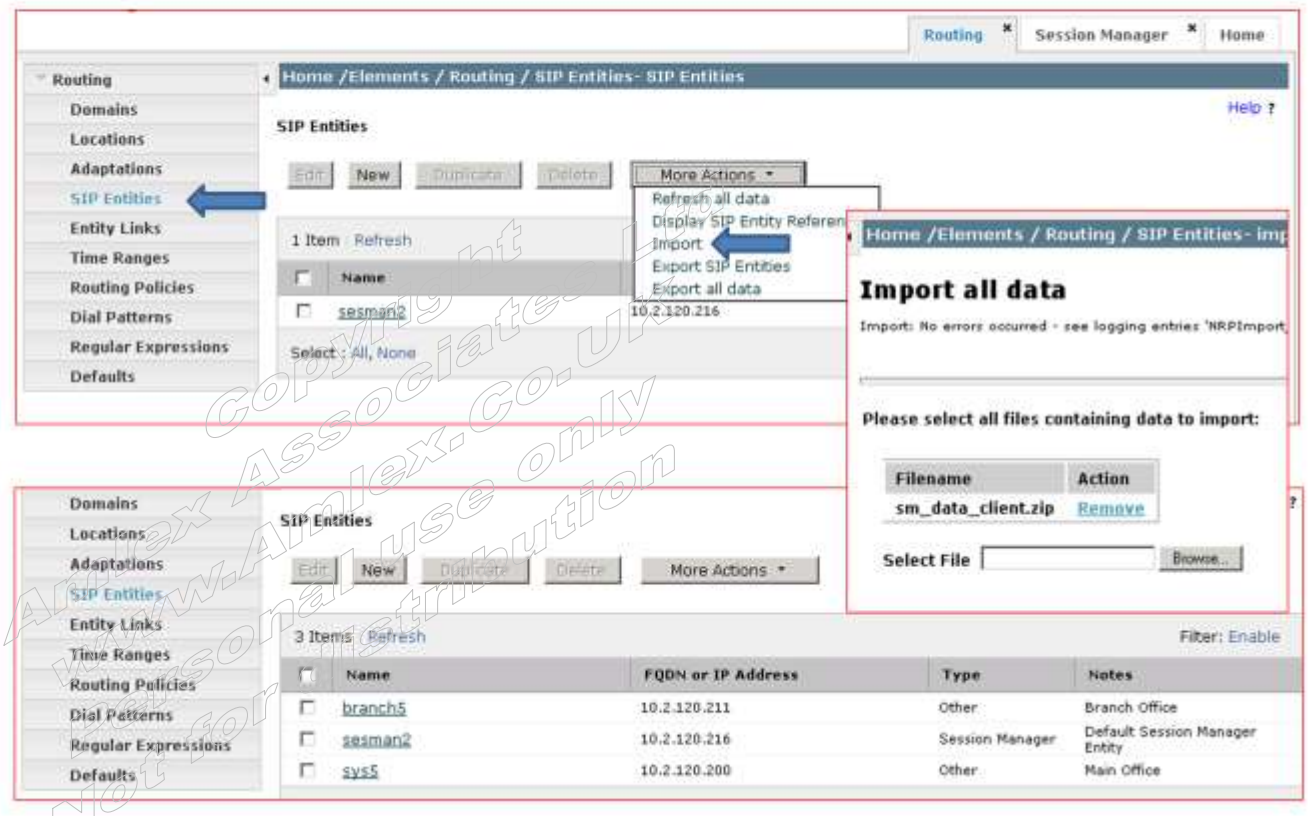
Copyright Amlex Associates Ltd

Import Database to Session Manager

Moving to the ROUTING section of the System Manager we select the **SIP ENTITIES** option and from that the **MORE ACTIONS** drop down menu to **IMPORT** the file created by the online tool. (**sm_data_client.zip**)

This will create the SIP Entities, Entity Links, Time Ranges Adaptions, Routing Policies, Dial Patterns etc for the SIP endpoints within the Session Manager.

Once the import is complete check that the SIP entities have been created and the Entity Links etc.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

275

Notes

_____

_____

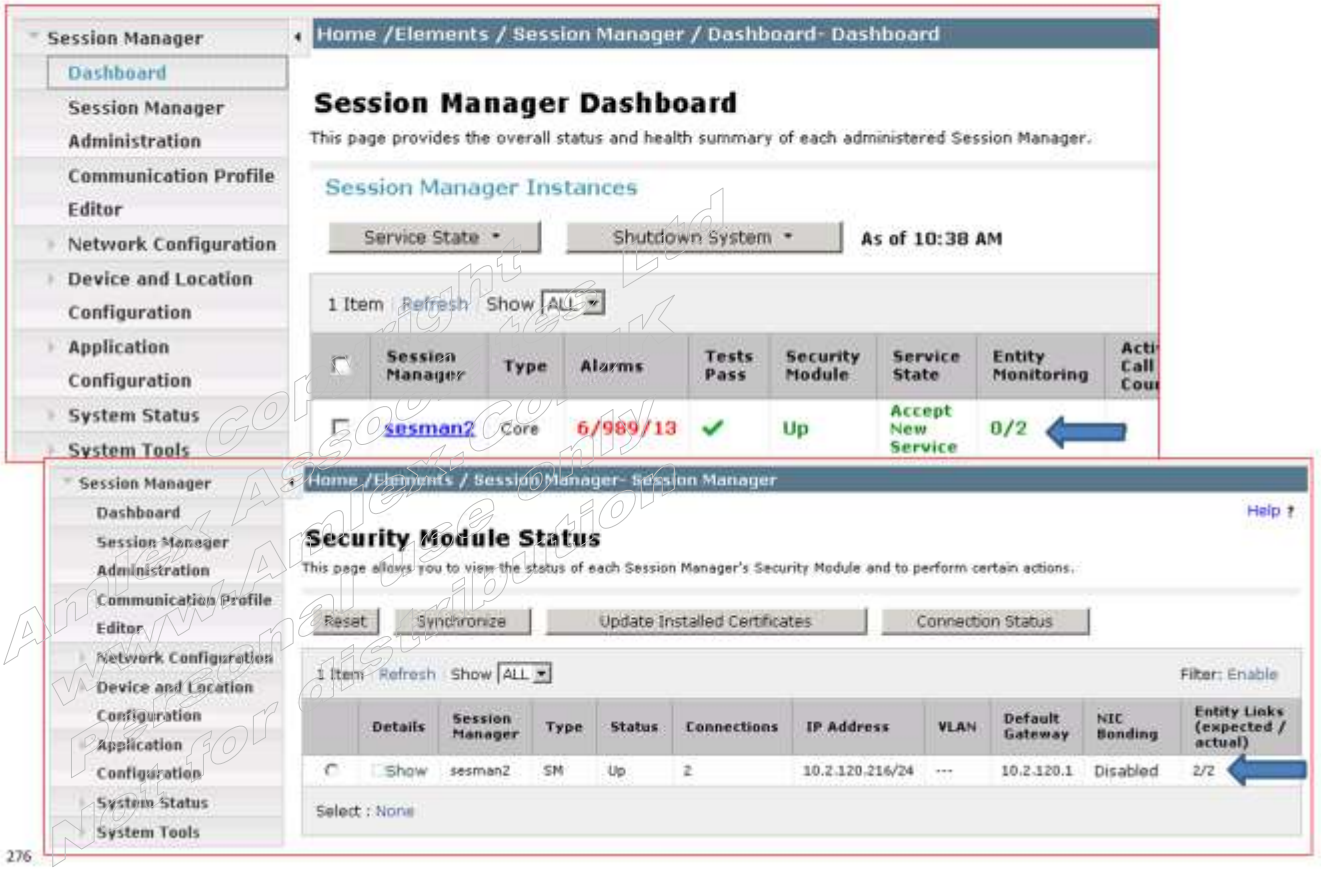
_____

_____

Check Entity Monitoring

Returning to the SESSION MANAGER DASHBOARD shown top we can now see that the number of Entities monitored is now 2 and that none are failing. (Top Arrow)

Also by clicking on the Security Module UP message we are taken to the Security Module Status shown below and on the far right is shows the Entity Links Expected and Actual. Again this is correct 2/2 i.e. Two links expected and in service.



Notes

_____

_____

_____

_____

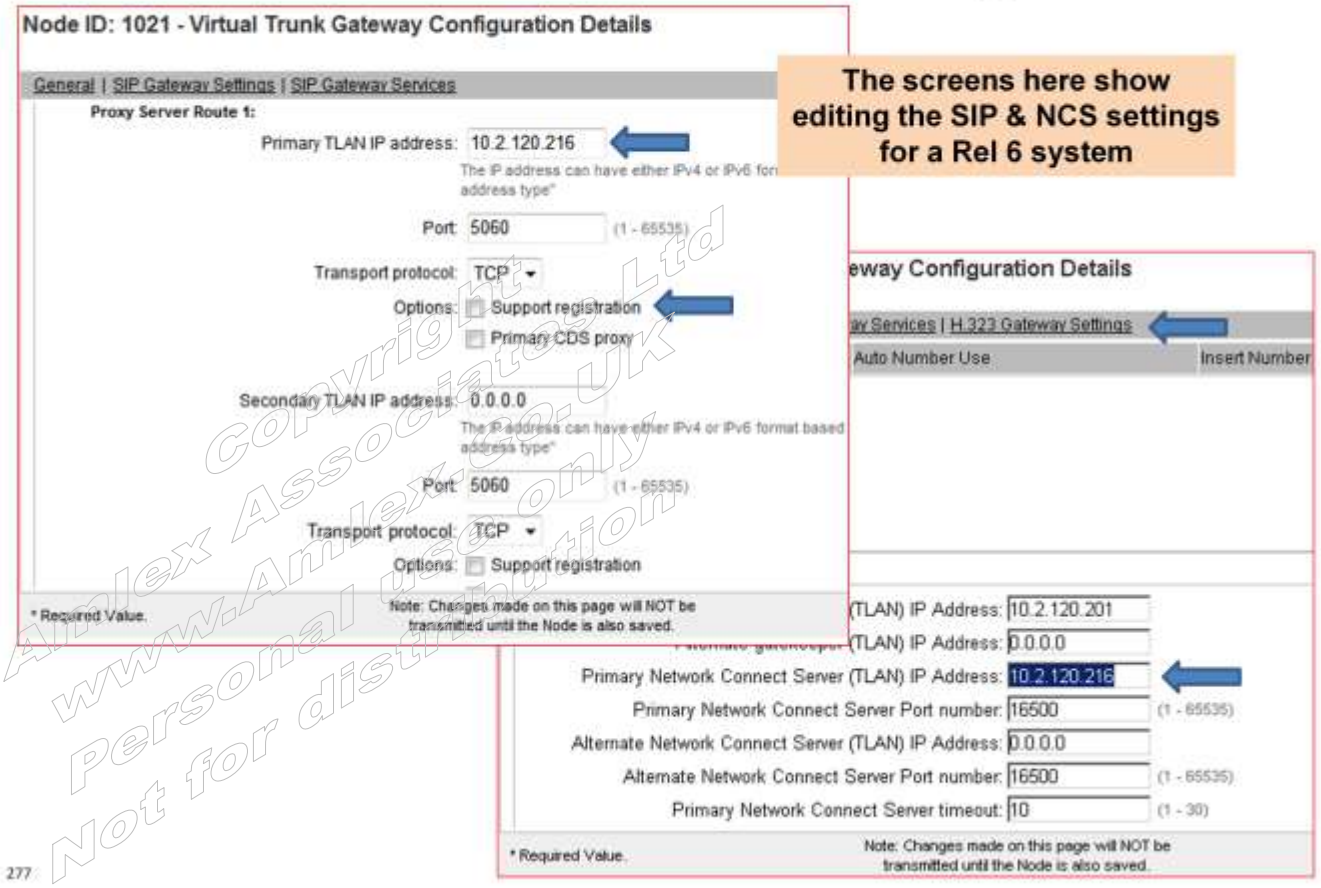
Copyright Amlex Associates Ltd

IP Node set to Session Mgr Rel 6

Next the IP Node information is edited on each of the CS1K systems to point to the Session Manger address so it uses that for call routing and redirection not the NRS.

Note that the SUPPORT REGISTRATION check box should be cleared as the Session Manager uses the Entity Link to monitor the end point rather than the registration request.

The lower screen shows the Network Connect Server setting which is associated with the H.323 Gateway settings on Rel 6.


Node ID: 1021 - Virtual Trunk Gateway Configuration Details
General | SIP Gateway Settings | SIP Gateway Services
Proxy Server Route 1:
Primary TLAN IP address: 10.2.120.216
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Primary CDS proxy
Secondary TLAN IP address: 0.0.0.0
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
* Required Value.
Note: Changes made on this page will NOT be transmitted until the Node is also saved.
The screens here show editing the SIP & NCS settings for a Rel 6 system
eway Configuration Details
ay Services | H.323 Gateway Settings
Auto Number Use
Insert Number
(TLAN) IP Address: 10.2.120.201
(TLAN) IP Address: 0.0.0.0
Primary Network Connect Server (TLAN) IP Address: 10.2.120.216
Primary Network Connect Server Port number: 16500 (1 - 65535)
Alternate Network Connect Server (TLAN) IP Address: 0.0.0.0
Alternate Network Connect Server Port number: 16500 (1 - 65535)
Primary Network Connect Server timeout: 10 (1 - 30)
* Required Value.
Note: Changes made on this page will NOT be transmitted until the Node is also saved.
277

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

Notes

_____

_____

_____

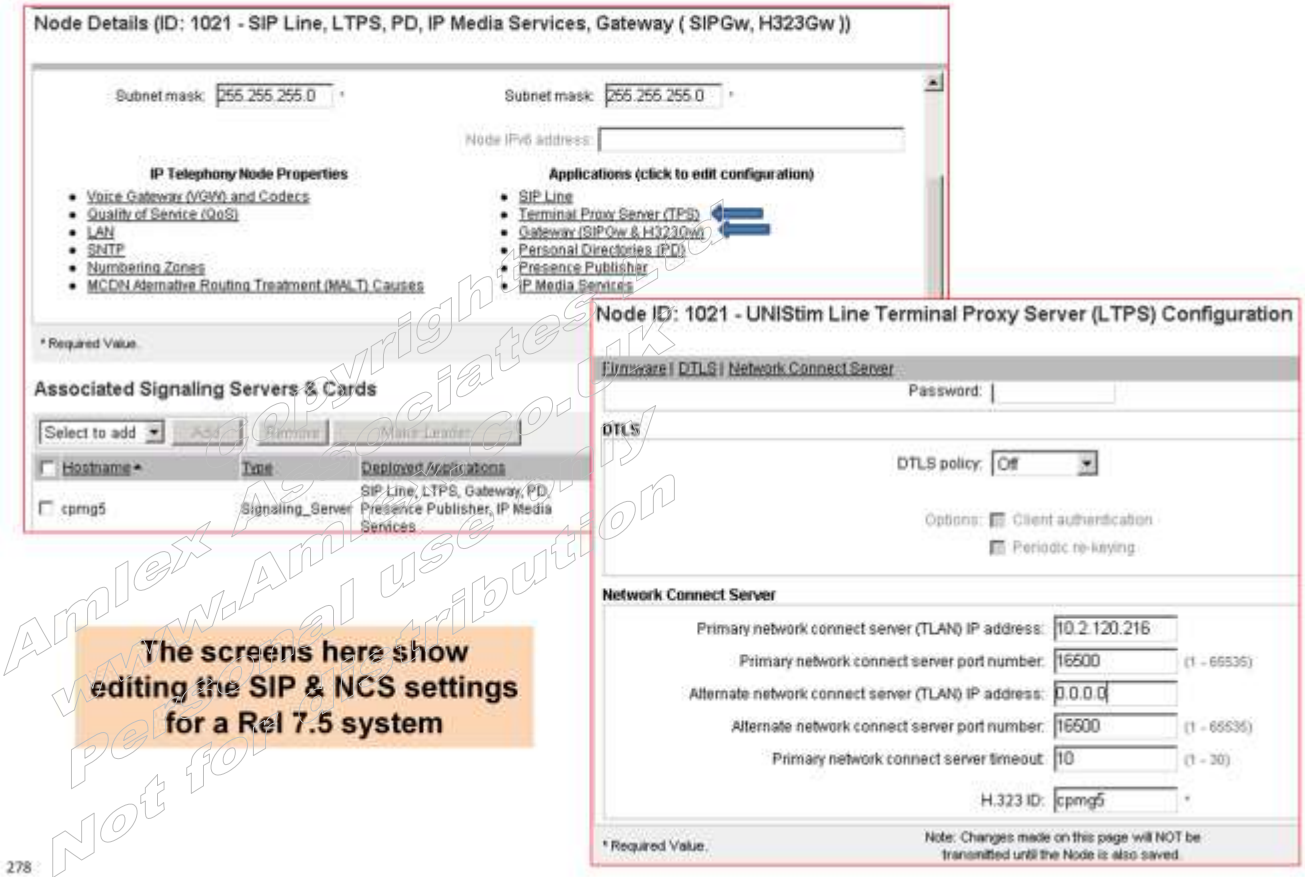
_____

IP Node set to Session Mgr Rel 7.5

The IP Node information is edited on each of the CS1K systems to point to the Session Manger address so it uses that for call routing and redirection not the NRS.

Select the TPS to edit the Network Connect Server setting first. Note the H323 ID is also part of the NCS setting as it is used as the name for the TPS Instance which is created on the Session Manager.

The lower screen shows the Network Connect Server setting which is associated with the H.323 Gateway settings on Rel 6.


Node Details (ID: 1021 - SIP Line, LTPS, PD, IP Media Services, Gateway (SIPGw, H323Gw))
Subnet mask: 255.255.255.0
Subnet mask: 255.255.255.0
Node IPv6 address:
IP Telephony Node Properties
Voice Gateway (VGW) and Codecs
Quality of Service (QoS)
LAN
SNTP
Numbering Zones
MCDN Alternative Routing Treatment (MALT) Causes
Applications (click to edit configuration)
SIP Line
Terminal Proxy Server (TPS)
Gateway (SIPGw & H323Gw)
Personal Directories (PD)
Presence Publisher
IP Media Services
* Required Value.
Associated Signaling Servers & Cards
Select to add
Add
Remove
Make Leader
Hostname
Type
Deployed Applications
cpmg5
Signaling_Server
SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services
Node ID: 1021 - UNIStim Line Terminal Proxy Server (LTPS) Configuration
Firmware | DTLS | Network Connect Server
Password:
DTLS
DTLS policy: Off
Options: Client authentication
Periodic re-keying
Network Connect Server
Primary network connect server (TLAN) IP address: 10.2.120.216
Primary network connect server port number: 16500 (1 - 65535)
Alternate network connect server (TLAN) IP address: 0.0.0.0
Alternate network connect server port number: 16500 (1 - 65535)
Primary network connect server timeout: 10 (1 - 30)
H.323 ID: cpmg5
* Required Value.
Note: Changes made on this page will NOT be transmitted until the Node is also saved.
278

The screens here show editing the SIP & NCS settings for a Rel 7.5 system

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

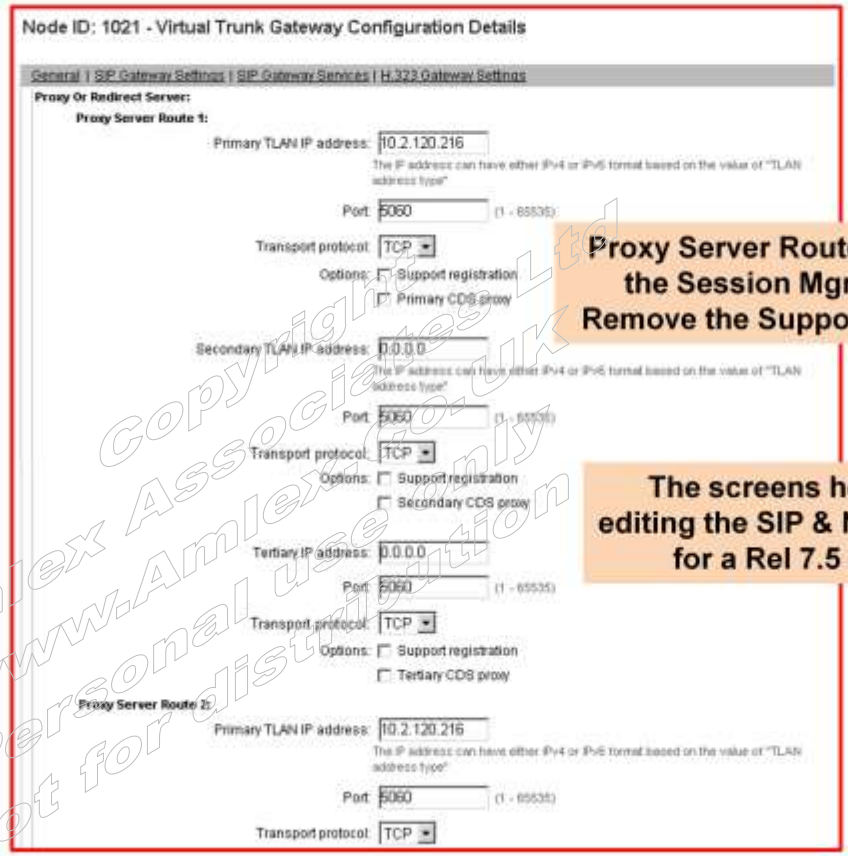
Copyright Amlex Associates Ltd

IP Node set to Session Mgr Rel 7.5

Both Proxy Server Route 1 & 2 need to be set to an address so we will point them to the SIP Entity address of the Session Manager.

Note the Secondary address is set to 0.0.0.0 and also the Port number is 5060. These cannot be left blank which can occur during an upgrade.

Note that the **SUPPORT REGISTRATION** check box should be cleared as the Session Manager uses the Entity Link to monitor the end point rather than the registration request.


Node ID: 1021 - Virtual Trunk Gateway Configuration Details
General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings
Proxy Or Redirect Server:
Proxy Server Route 1:
Primary TLAN IP address: 10.2.120.216
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Primary CDS proxy
Secondary TLAN IP address: 0.0.0.0
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Secondary CDS proxy
Tertiary IP address: 0.0.0.0
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Tertiary CDS proxy
Proxy Server Route 2:
Primary TLAN IP address: 10.2.120.216
Port: 5060 (1 - 65535)
Transport protocol: TCP
Proxy Server Route 1 & 2 are changed to the Session Mgr SIP Entity Address
Remove the Support Registration setting.
The screens here show editing the SIP & NCS settings for a Rel 7.5 system

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

279

Notes

_____

_____

_____

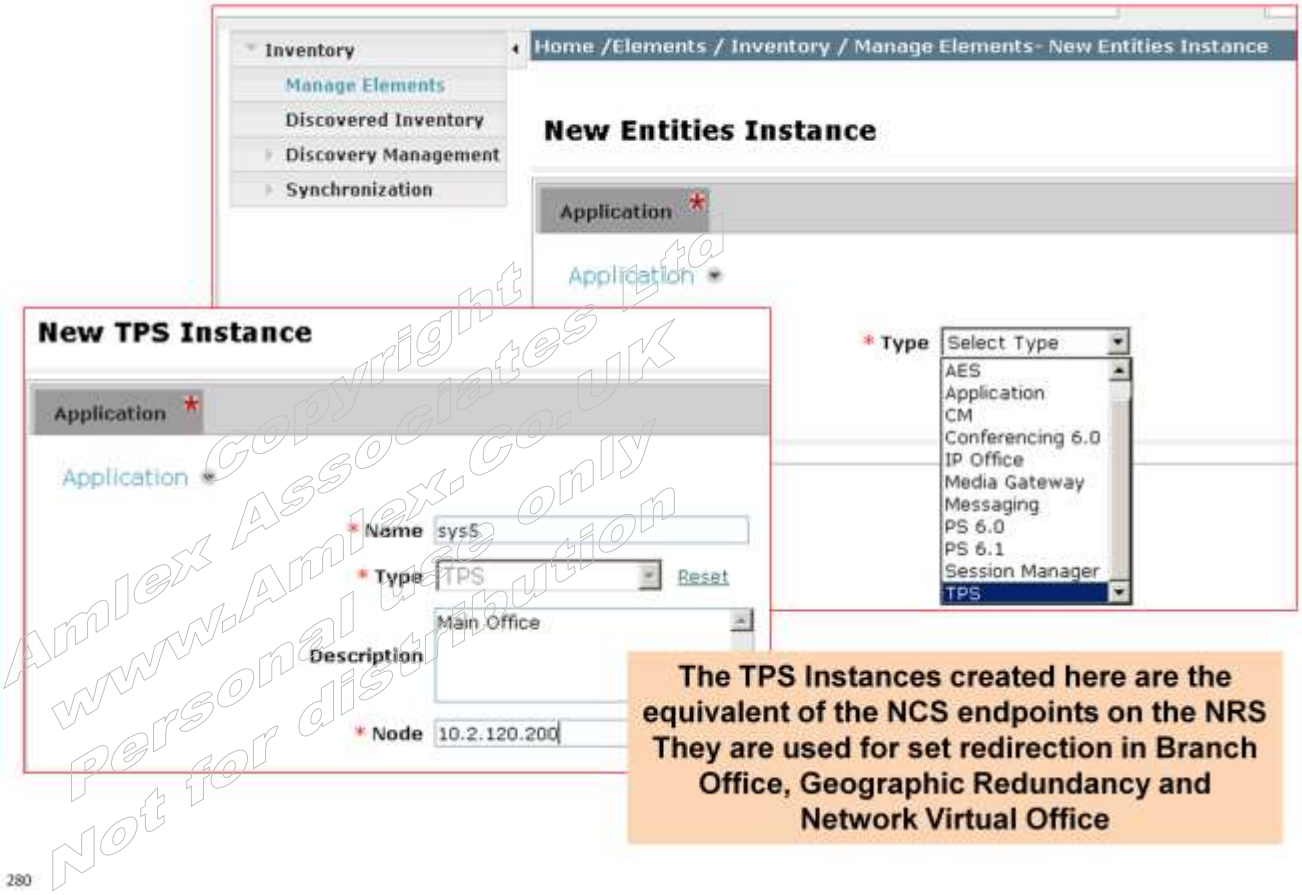
_____

Back on the System Manager we need to create TPS Instances in the **INVENTORY** section for NCS redirections .

This is because on the NRS the endpoint for each system allows routing for SIP, H323 and UniStim requests. However on the Session Manager this is not the case. The SIP Entity is used for SIP routing but for the UniStim (NCS) requests we need to add a separate TPS Instance.

Each system is created as a TPS Instance as shown here. The name used is the H323 ID for the specific system.

Create New TPS Instance



Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

NRS Proxy Users (NCS Routing)

Once the TPS instances are created we then need to apply some routing information for the redirections.

Again on the NRS this was all done through one route entry but this is not the case on the System/Session manager.

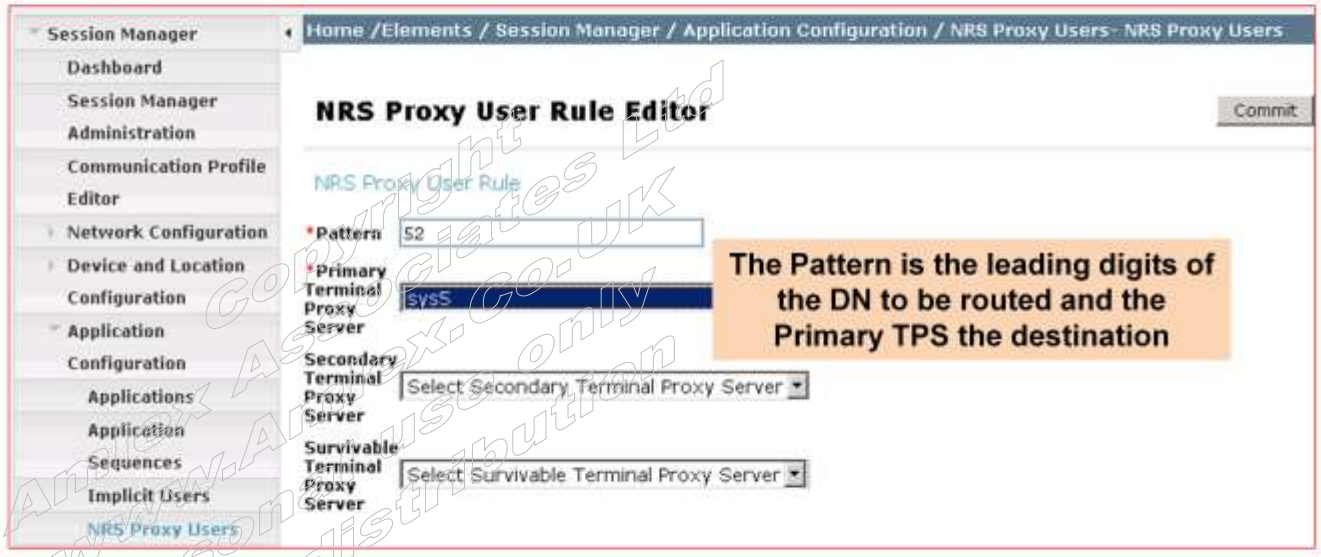
To add the relevant Route pattern go to:-

SESSION MANAGER / APPLICATION CONFIGURATION / NRS PROXY USERS

Patterns are added as shown selecting the destination from the drop down menus as shown.

Here we are adding 52, so for sets with DN's in the range 52xx when they make redirection requests they will be sent to the system **sys5**.

With the SIP & NCS now reset the calls should now be routing via the Session Manager.


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
Applications
Application Sequences
Implicit Users
NRS Proxy Users
Home /Elements / Session Manager / Application Configuration / NRS Proxy Users- NRS Proxy Users
NRS Proxy User Rule Editor
Commit
NRS Proxy User Rule
*Pattern 52
*Primary Terminal Proxy Server sys5
Secondary Terminal Proxy Server Select Secondary Terminal Proxy Server
Survivable Terminal Proxy Server Select Survivable Terminal Proxy Server
The Pattern is the leading digits of the DN to be routed and the Primary TPS the destination

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

281

Notes

_____

_____

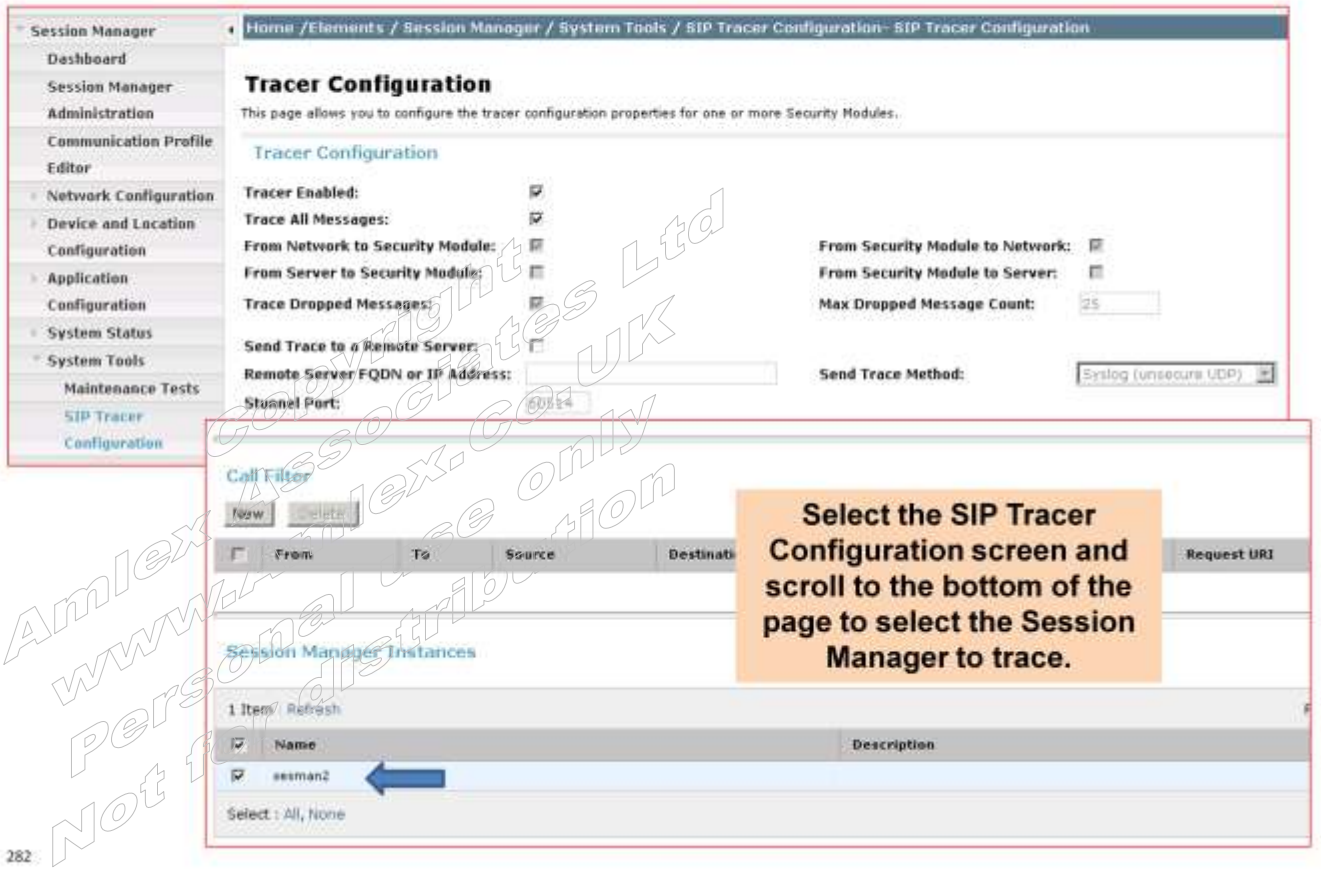
_____

_____

Session Manager Tracer Configuration

SIP trace information can be obtained from the Session Manager itself and also viewed there. It must first be setup correctly so on the Session Manager tab in System Manager select SIP Tracer Configuration from the System Tools area.

Generally the default options will suffice and there is also the possibility to add Filters to the output. However one thing that must be done is to select the Session Manager instance to trace. This is done at the very bottom of the screen as shown here.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

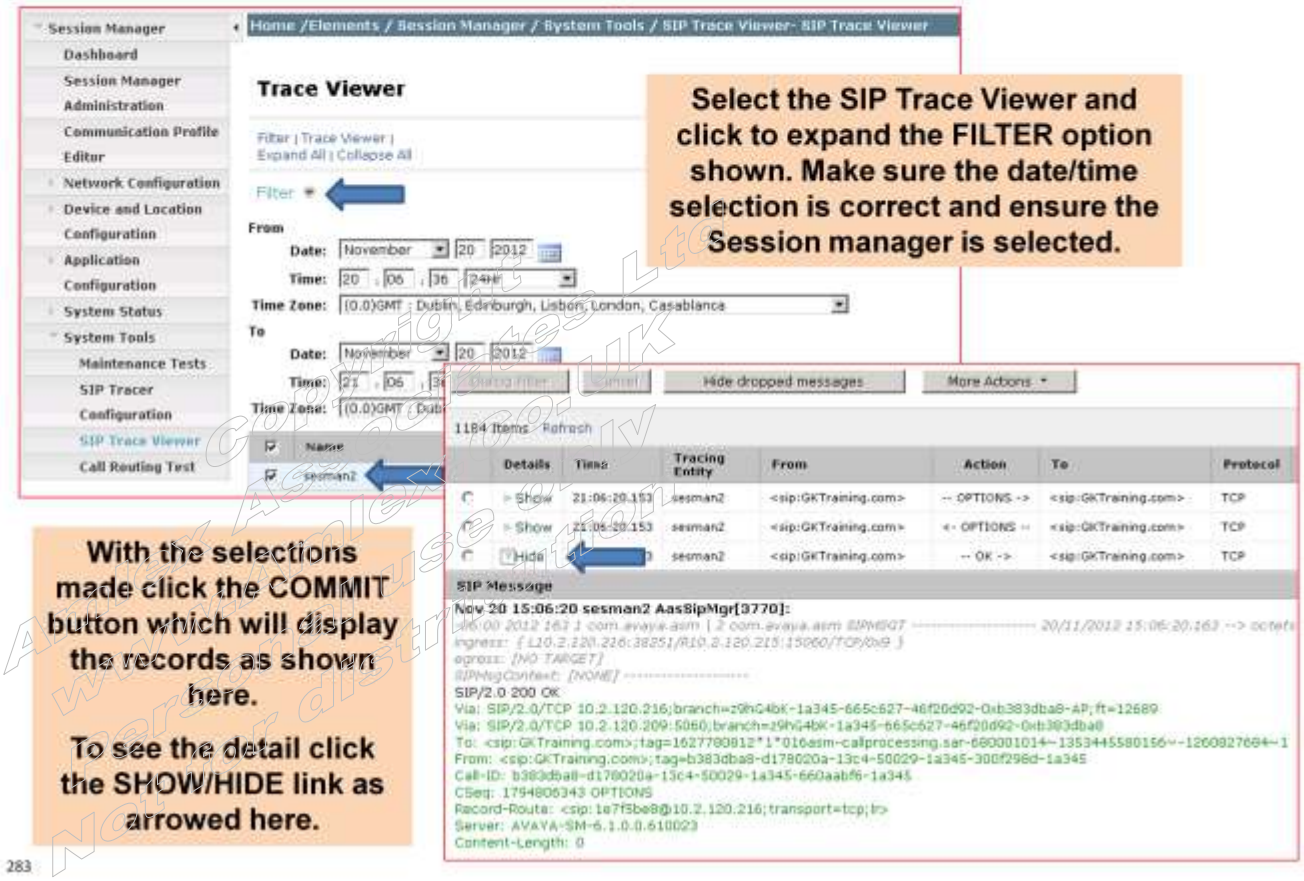
Session Manager Trace Viewer

To display the Trace information first you need to access the **TRACE VIEWER** screen as shown here.

When first opened you need to add the **FILTER** for the time/date and also to check the box for the Session Manager you are tracing.

With this information added you can click the COMMIT button to view the Trace records selected by the FILTER applied earlier.

To look at the detail of a specific record you simply click on the SHOW / HIDE link as arrowed in the lower screen shot.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

traceSM on Session Manager

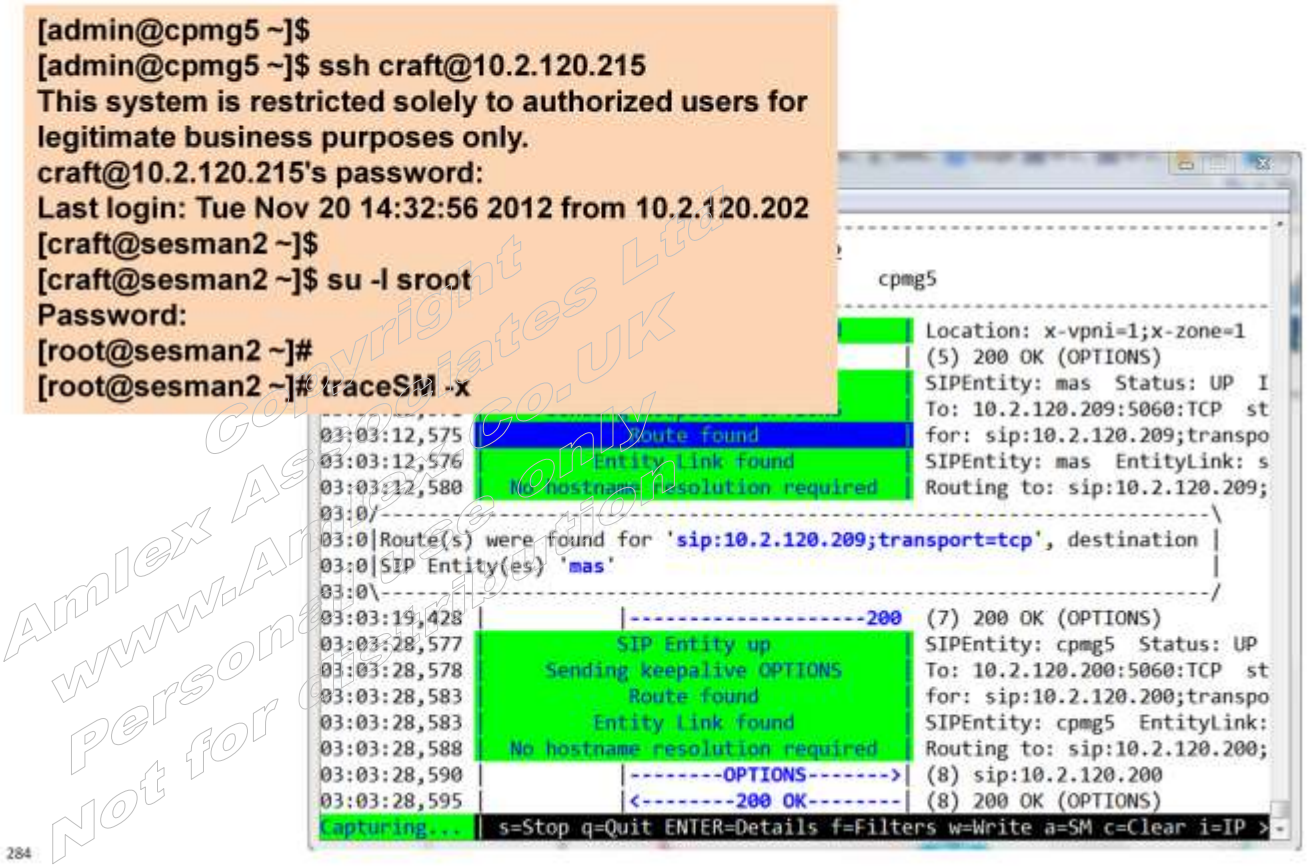
The SIP tracing command on the Session Manager is **traceSM** and it needs to be run from the **sroot** account.

The example here shows a session being created by logging into the Management IP address of the Session Manager using SSH from another Linux system. It is also possible to use a tool such as **puTTy** to login directly to the Session Manager.

To login across the network you will need to use the "**craft**" account to gain access and then switch user to the privileged user "**sroot**".

Once at this level the command **traceSM -x** is issued to start the trace function (Note:- the –x option is used to stop **traceSM** loading the previous log file which can take some time). The command contains help information but to start the capture simply type "**s**" and "**s**" again to stop it.

Use the **UP** & **DOWN** arrows to scroll through the capture and the **RETURN** to inspect the detail.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Make System Manager Primary UCM

In order to use the System Manager the Primary UCM we First have to turn UCM on.

This is done by navigating to the shown page:-

CONFIGURATIONS / SETTINGS / SMGR / COMMON CONSOLE.

Here you need to edit the setting

ucm_configured

and set it to **true**.

After committing the change you will need to logout and log back in again to the System Manager to see the UCM Services option on the dashboard.

This enables display of the UCM Services Menu option on the System Manager dashboard

Amlex Copyright www.Amlex.Associates Ltd Personal use only Not for distribution

285

Notes

_____

_____

_____

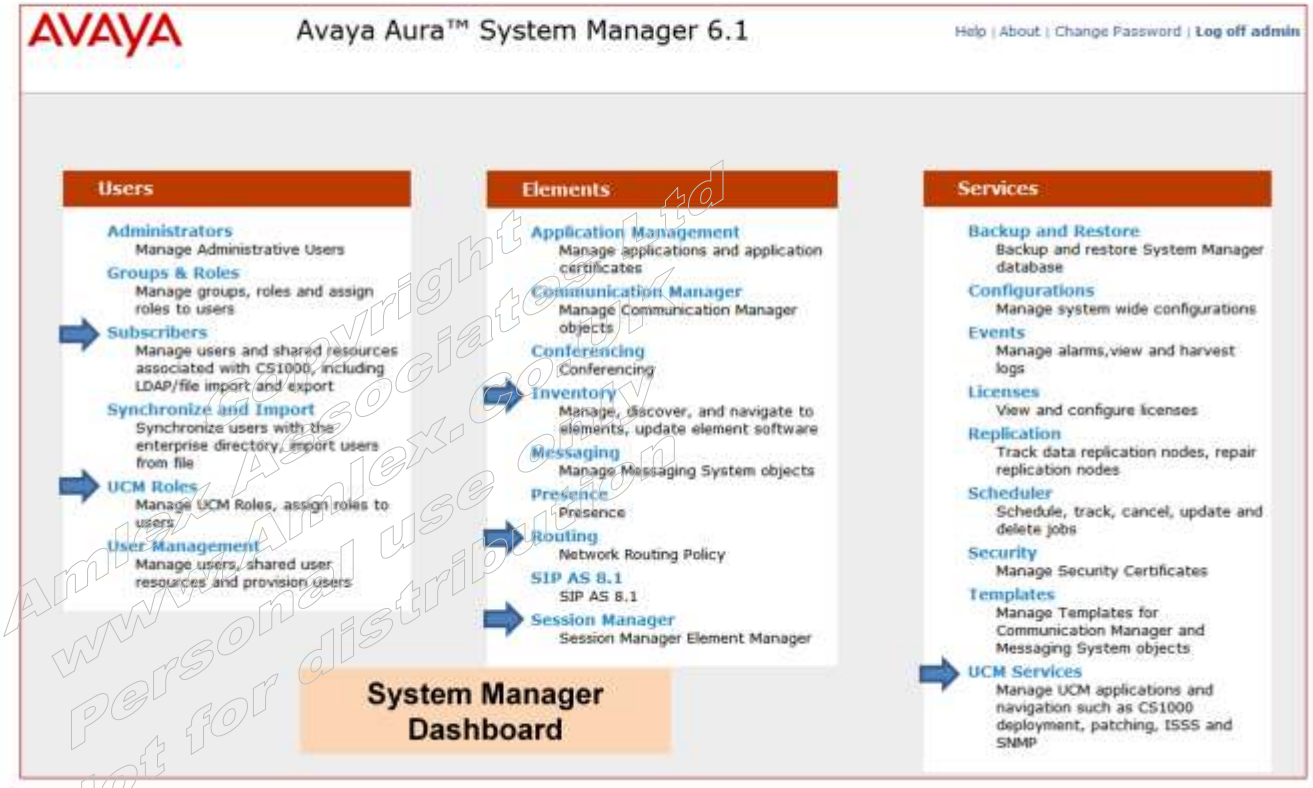
_____

System Manager with UCM

Once the UCM is enabled the System Manager display should be as shown.

Clicking on the UCM SERVICES option will take you to the standard UCM Elements page shown on the following page.

Note also the addition of UCM Roles and SUBSCRIBERS to the USERS section of the System Manager dashboard.



Amlex Copyright Associates Ltd www.Amlex.com Personal use only Not for distribution

Notes

_____

_____

_____

_____

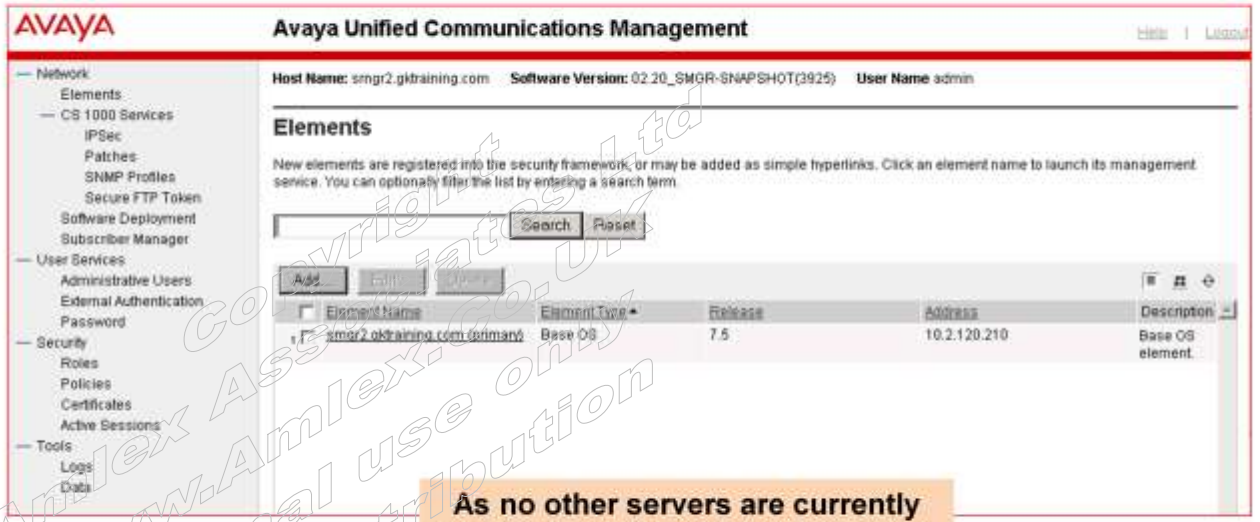
UCM Elements

This is the UCM Elements page you will see on a new system with no servers registered.

Note the similarity to the CS1K UCM and the System Manager Element shown in the list.

One significant difference is that the Element type for the System Manager is Base OS rather than Linux Base.

Thus clicking on the link will return you to the System Manager rather than the Linux Base as it would with a CS1K UCM primary server.



As no other servers are currently registered to the System Manager only its own entry as BASE OS is seen at this point.

Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

287

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add Software loads & Linux to UCM

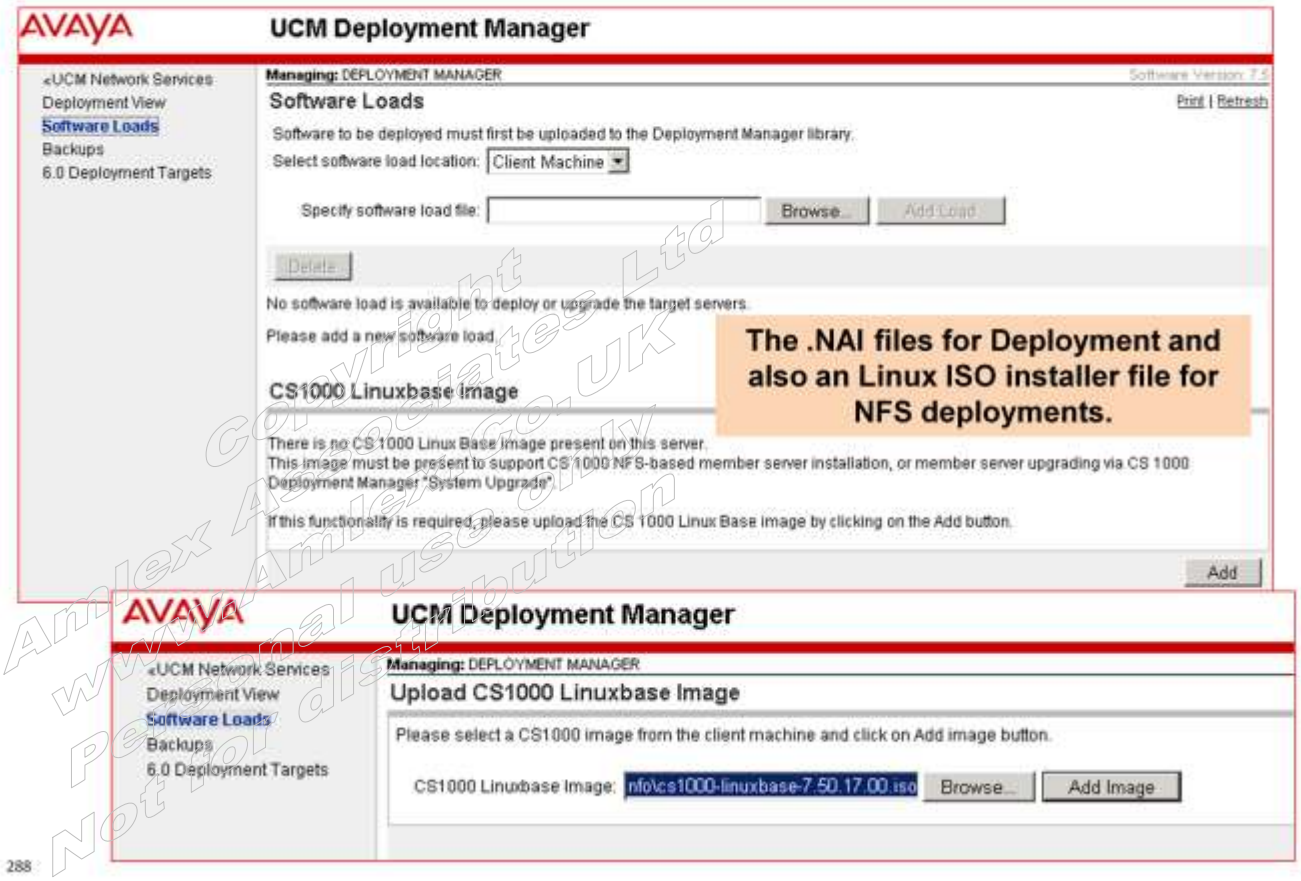
Similar to a new installation one of the first things to do is to add the Deployment loads (.NAI) files to the UCM .

As with a CS1K based system you will need to enter the credentials to be used for Deployment on the first access to the Deployment Manager.

Once this is done you can proceed to add the relevant .nai files .

In addition you need to upload the Linux ISO file for installations that install both the Linux and Applications. (NFS Install option)

This is not needed on a CS1K installation as it is done during the installation of the Deployment server itself.


AVAYA
UCM Deployment Manager
<UCM Network Services
Deployment View
Software Loads
Backups
6.0 Deployment Targets
Managing: DEPLOYMENT MANAGER
Software Version: 7.5
Software Loads
Print | Refresh
Software to be deployed must first be uploaded to the Deployment Manager library.
Select software load location: Client Machine
Specify software load file:
Browse...
Add Load
Delete
No software load is available to deploy or upgrade the target servers.
Please add a new software load.
CS1000 Linuxbase Image
There is no CS 1000 Linux Base image present on this server.
This image must be present to support CS 1000 NFS-based member server installation, or member server upgrading via CS 1000 Deployment Manager "System Upgrade".
If this functionality is required, please upload the CS 1000 Linux Base image by clicking on the Add button.
Add
The .NAI files for Deployment and also an Linux ISO installer file for NFS deployments.
AVAYA
UCM Deployment Manager
<UCM Network Services
Deployment View
Software Loads
Backups
6.0 Deployment Targets
Managing: DEPLOYMENT MANAGER
Upload CS1000 Linuxbase Image
Please select a CS1000 image from the client machine and click on Add image button.
CS1000 Linuxbase Image:
nfo\cs1000-linuxbase-7.50.17.00.iso
Browse...
Add Image
288

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Register Rel 6 Server to System Mgr

Once the software has been uploaded to the server you can proceed with re-registering the existing Rel 6 CS1K servers to the System Manager as the new Primary UCM.

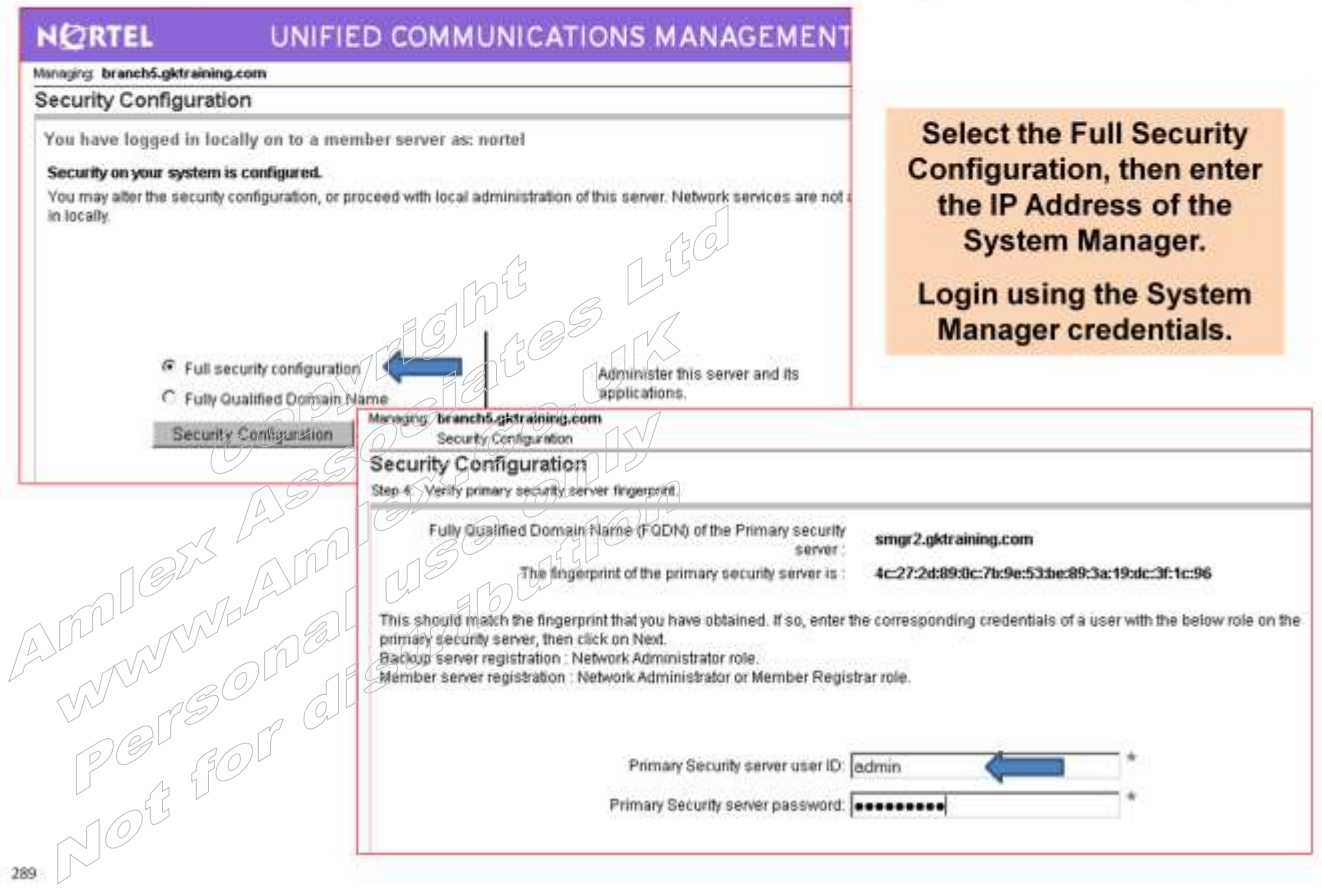
To do this we browse to the server using the local login option e.g. :-

https://branch5.gktraining.com/local-login

Login with the nortel account (Rel 6) and select Full Security Configuration.

When asked for the location of the Primary UCM enter the IP address of the System manager.

Note the FQDN of the System Manager and fingerprint in the lower display.


NORTEL UNIFIED COMMUNICATIONS MANAGEMENT
Managing: branch5.gktraining.com
Security Configuration
You have logged in locally on to a member server as: nortel
Security on your system is configured.
You may alter the security configuration, or proceed with local administration of this server. Network services are not
in locally.
Full security configuration
Administer this server and its applications.
Fully Qualified Domain Name
Security Configuration
Select the Full Security Configuration, then enter the IP Address of the System Manager.
Login using the System Manager credentials.
Managing: branch5.gktraining.com
Security Configuration
Security Configuration
Step 4 - Verify primary security server fingerprint
Fully Qualified Domain Name (FQDN) of the Primary security server : smgr2.gktraining.com
The fingerprint of the primary security server is : 4c:27:2d:89:0c:7b:9e:53:be:89:3a:19:dc:3f:1c:96
This should match the fingerprint that you have obtained. If so, enter the corresponding credentials of a user with the below role on the primary security server, then click on Next.
Backup server registration : Network Administrator role.
Member server registration : Network Administrator or Member Registrar role.
Primary Security server user ID: admin
Primary Security server password:
289

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Re-Registered Server on UCM

With the CS1K systems registered to the System manager they will now show up in the Elements table as shown here and also in the Deployment view as shown below.

You can now complete the Deployment of the servers to be upgraded as you would on a standard CS1K system.

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

290

Notes

_____

_____

_____

_____

Register Rel 7.5 Server to System Mgr

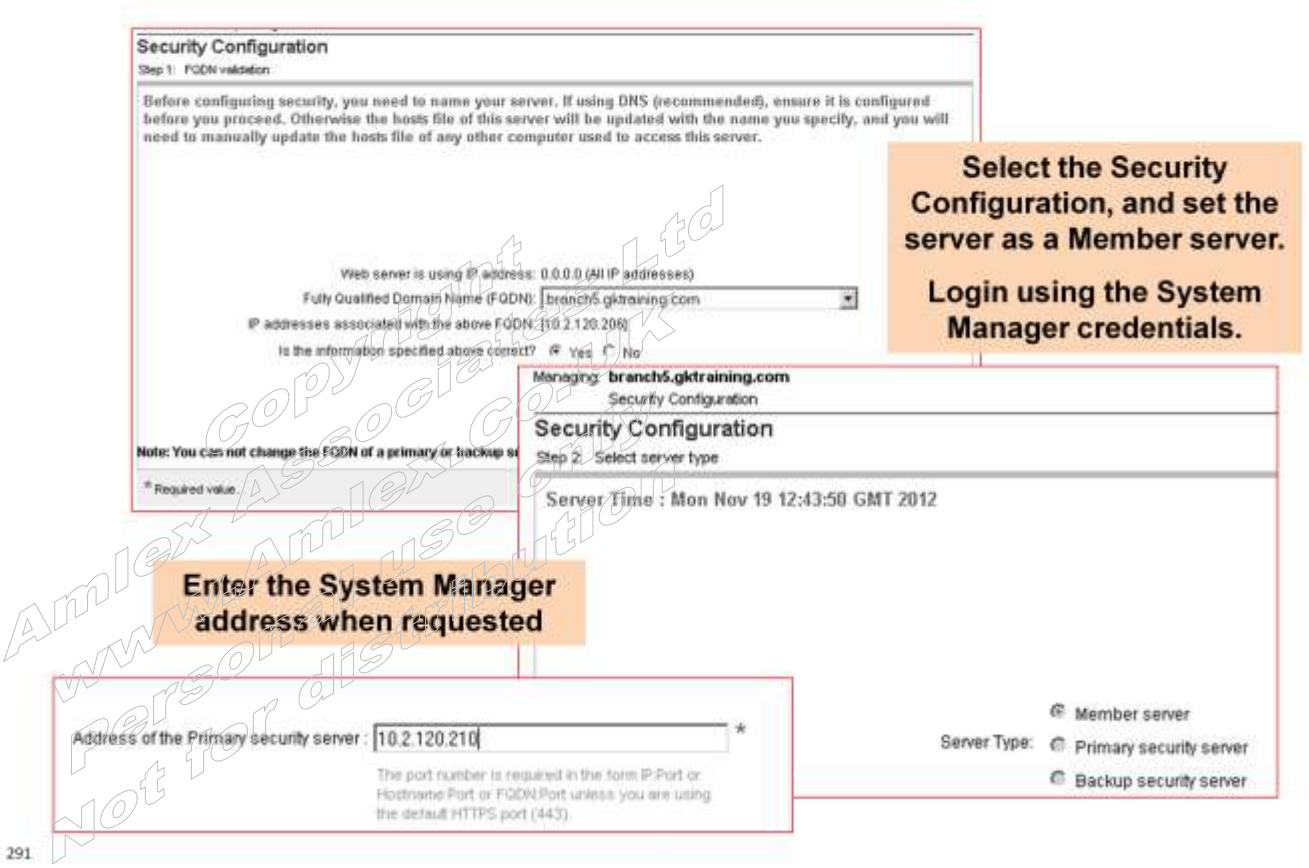
When re-registering systems to the System Manager it is wise to start with the Member and Backup servers and finish with the Primary UCM server.

To re-register the system browse to the server using the local login option e.g. :-

https://branch5.gktraining.com/local-login

Login with the admin2 account (Rel 7.5) and select Security Configuration or Demote Server in the case of a Primary UCM server.

The server type will always be a Member and when prompted for the address of the Primary server enter the System Manager IP.


Security Configuration
Step 1: FQDN validation
Before configuring security, you need to name your server. If using DNS (recommended), ensure it is configured before you proceed. Otherwise the hosts file of this server will be updated with the name you specify, and you will need to manually update the hosts file of any other computer used to access this server.
Web server is using IP address: 0.0.0.0 (All IP addresses)
Fully Qualified Domain Name (FQDN): branch5.gktraining.com
IP addresses associated with the above FQDN: 10.2.120.206
Is the information specified above correct? Yes No
Select the Security Configuration, and set the server as a Member server.
Login using the System Manager credentials.
Managing: branch5.gktraining.com
Security Configuration
Security Configuration
Step 2: Select server type
Server Time : Mon Nov 19 12:43:50 GMT 2012
Enter the System Manager address when requested
Address of the Primary security server : 10.2.120.210 *
The port number is required in the form IP:Port or Hostname:Port or FQDN:Port unless you are using the default HTTPS port (443).
Server Type: Member server
Primary security server
Backup security server
* Required value
291

Notes

_____

_____

_____

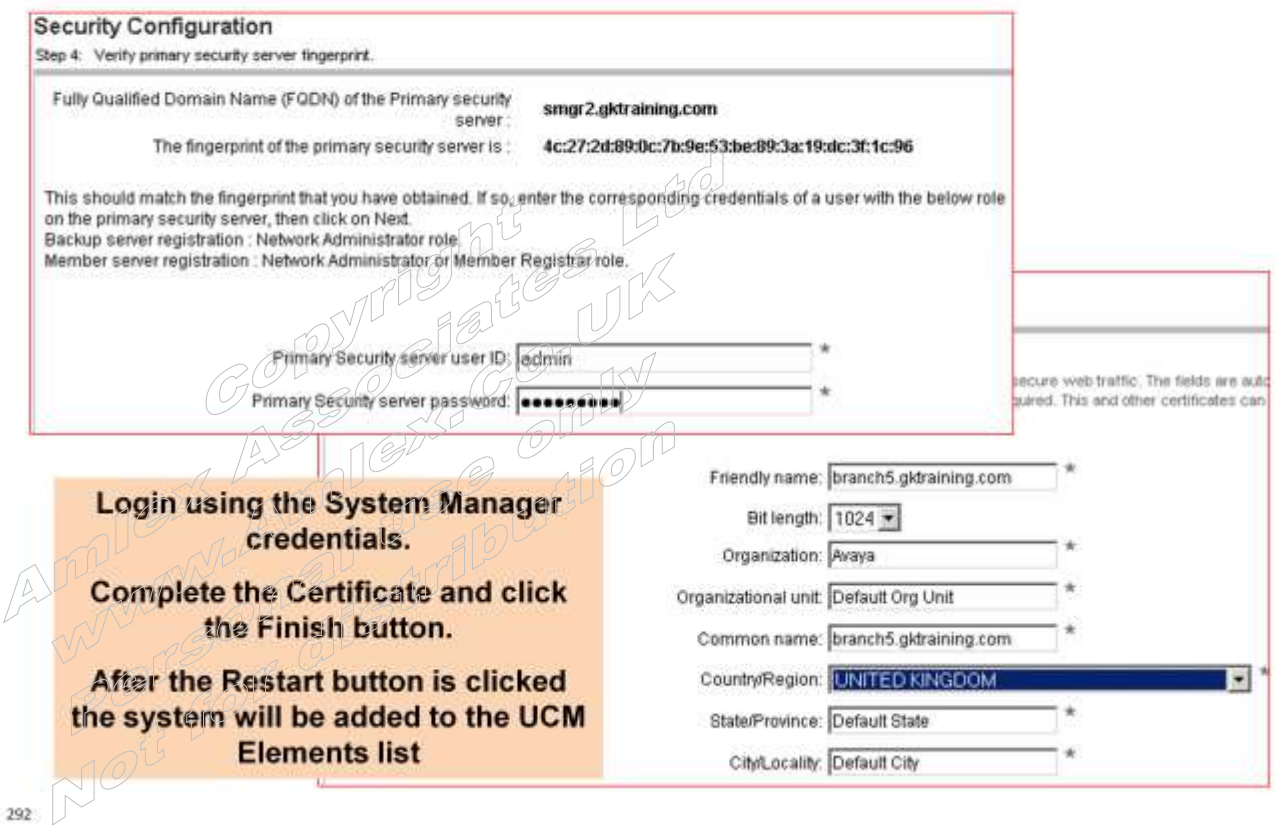
_____

Copyright Amlex Associates Ltd

Register Rel 7.5 Server to System Mgr

Login with the System Manager credentials and edit the Certificate setting as required before clicking the Finish button and subsequently the Restart button.

The system will appear in the UCM Elements list after the restart


Security Configuration
Step 4: Verify primary security server fingerprint.
Fully Qualified Domain Name (FQDN) of the Primary security server :
smgr2.gktraining.com
The fingerprint of the primary security server is :
4c:27:2d:89:0c:7b:9e:53:be:89:3a:19:dc:3f:1c:96
This should match the fingerprint that you have obtained. If so, enter the corresponding credentials of a user with the below role on the primary security server, then click on Next.
Backup server registration : Network Administrator role.
Member server registration : Network Administrator or Member Registrar role.
Primary Security server user ID: admin
Primary Security server password:
Friendly name: branch5.gktraining.com
Bit length: 1024
Organization: Avaya
Organizational unit: Default Org Unit
Common name: branch5.gktraining.com
Country/Region: UNITED KINGDOM
State/Province: Default State
City/Locality: Default City
Login using the System Manager credentials.
Complete the Certificate and click the Finish button.
After the Restart button is clicked the system will be added to the UCM Elements list
292

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

24. PRI Trunks

The key part of the TDM trunks is the PRI card itself. There are several different configurations of card but for CS1000 systems it tends to be the NTBK50 which has the option of two daughter boards which support the Clock Controller and the D-Channel interface.

The Clock controller is necessary for to ensure the correct synchronisation of timeslots. One card can support multiple links but they must be housed in the same Media Gateway on a CS1000. Hence you are likely to see multiple PRI cards in a chassis with only one equipped with a Clock controller (MGCLK).

The D-Channel card interfaces the system to the circuit and generates and interprets the signalling messages for the link.

NTBK50 2.0 Mb PRI

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

293

Notes

_____

_____

_____

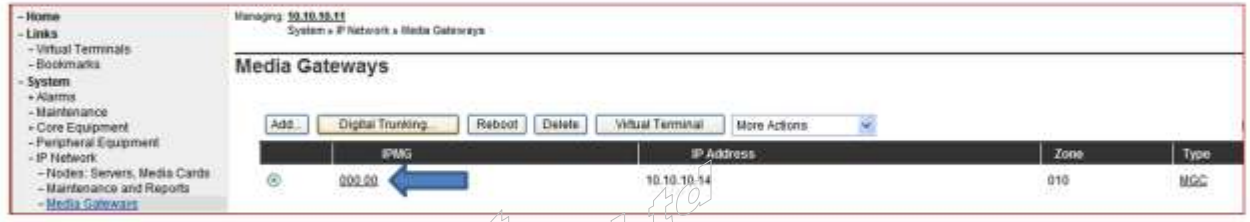
_____

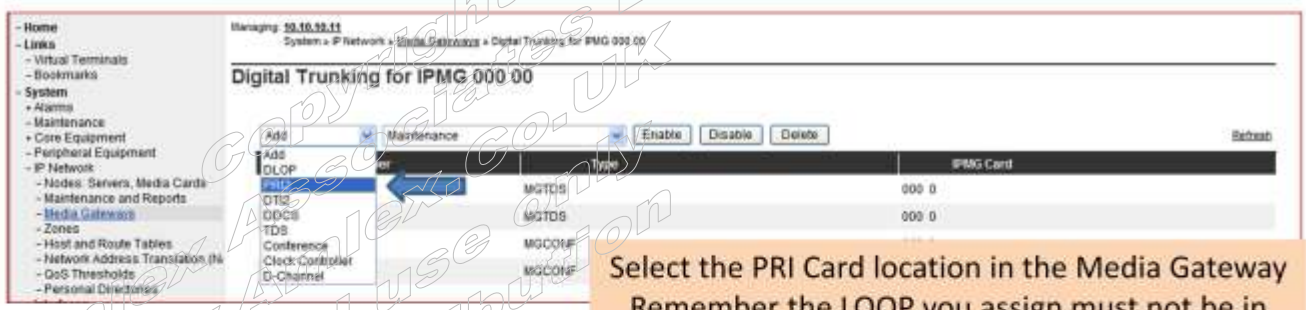
Assign LOOP to PRI Card

ISDN has already been configured so we can move on to configuring the PRI card with a LOOP number.

To configure the PRI LOOP number, first select the Media Gateway it is installed in, and click the **DIGITAL TRUNKING** button. Then select **PRI2** from the **ADD** drop down menu.

The system will prompt for a LOOP number to assign to the PRI. This must be an unused LOOP number and is not part of any existing SUPERLOOP. Here we have selected LOOP 100.





Select the PRI Card location in the Media Gateway
Remember the LOOP you assign must not be in use for any other SUPERLOOP or Device.

294

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

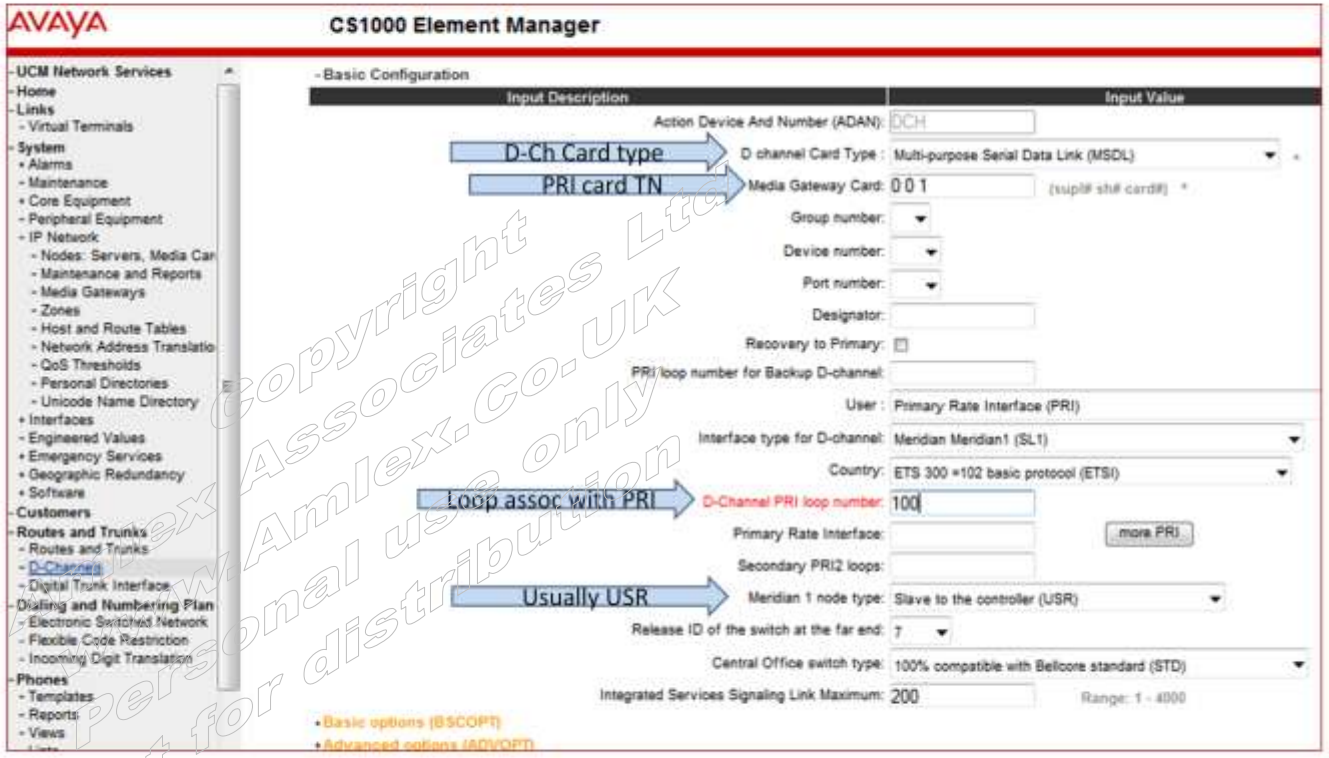
D-Channel

The figure shows a D-Channel configuration screen for a PRI card.

Note that in the D-Channel we are stating which DCH card is being used and as ours are daughter boards on the PRI itself the location (MG_CARD) is the same as the PRI e.g. 000 0 1 i.e. where the card is located in the Media Gateway.

As the trunks we are configuring are connecting together CS1K systems we have selected User(USR) as PRI and the Interface type for D-channel (IFC) as SL1. If you were configuring this to a different type of system or to the PSTN this would need to be selected appropriately.

Again as we are working “Back to Back” with another system we must define one end as NET and the other as USR as shown here (default). In a PSTN scenario the carrier end would always be NET so you would select USR.



Amlex Copyright
Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

295

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Route

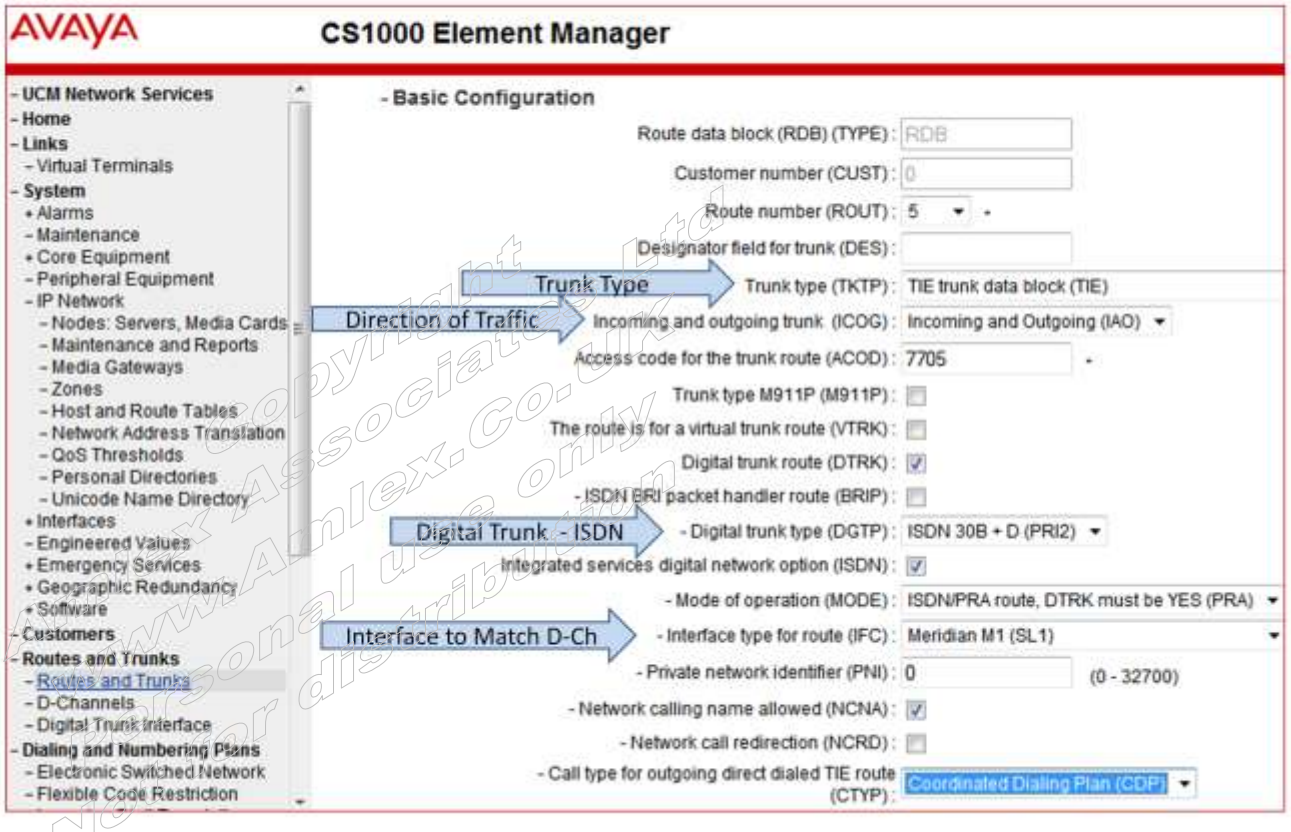
Here we are looking at the configuration of the Route itself.

Note the Trunk type has been set to TIE, as similar to the previous D-Channel example, this route is being configured to connect to another Meridian/CS1000 system.

The ACOD or Access Code is a number assigned to all routes which allows it to be selected directly from a set. (Set requires correct Privilege). It can be useful for testing and diagnostics.

The Digital Trunk type has been set to ISDN 30B+D (PRI2) the common European standard. Also the interface has been set to SL1 to match the D-Channel configuration. As the systems being joined are both Meridian using SL1 allows us to send the maximum feature information.

The Highlighted item shown is the default call type for this route if none is selected. We've chosen CDP the Coordinated Dial Plan which is most common in CS1K systems.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 0
Route number (ROUT) : 5
Designator field for trunk (DES) :
Trunk Type
Trunk type (TKTP) : TIE trunk data block (TIE)
Direction of Traffic
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7705
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
Digital trunk route (DTRK) :
- ISDN BRI packet handler route (BRIP) :
Digital Trunk - ISDN
- Digital trunk type (DGTP) : ISDN 30B + D (PRI2)
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : ISDN/PRA route, DTRK must be YES (PRA)
Interface to Match D-Ch
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 0 (0 - 32700)
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- Call type for outgoing direct dialed TIE route (CTYP) : Coordinated Dialing Plan (CDP)

296

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

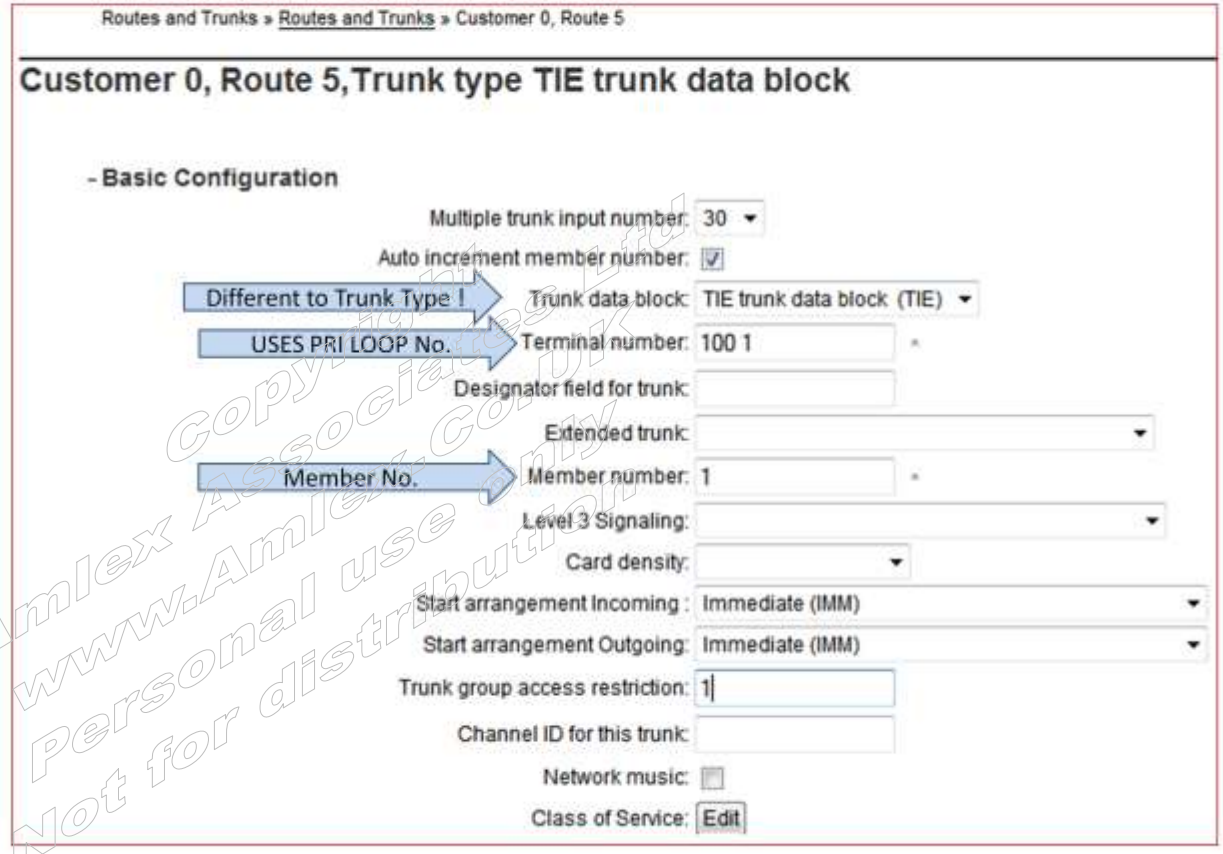
Trunks

The trunks themselves are the individual channels in the PRI connection to carry the voice. So here we are creating 30 (ISDN 30 B + D) trunks for our route.

Note that the Trunk Data Block is different from the Trunk Type selected for the route although it is still selected as a TIE here. If this had been a Virtual Trunk the TYPE would have been IPTI even though the Route Trunk Type would still have been TIE.

Note the TN here can be confusing especially for PRI's as we use the LOOP number rather than the Card TN. The Link is created when we designate the PRI2 Loop associated with the physical card.

The Member number is literally just that. The Trunk Member number starting at 1 and rising to 30.


Routes and Trunks » Routes and Trunks » Customer 0, Route 5
Customer 0, Route 5,Trunk type TIE trunk data block
- Basic Configuration
Multiple trunk input number: 30
Auto increment member number:
Different to Trunk Type !
Trunk data block: TIE trunk data block (TIE)
USES PRI LOOP No.
Terminal number: 100 1
Designator field for trunk:
Extended trunk:
Member No.
Member number: 1
Level 3 Signaling:
Card density:
Start arrangement Incoming : Immediate (IMM)
Start arrangement Outgoing: Immediate (IMM)
Trunk group access restriction: 1
Channel ID for this trunk:
Network music:
Class of Service: Edit

297

Notes

_____

_____

_____

_____

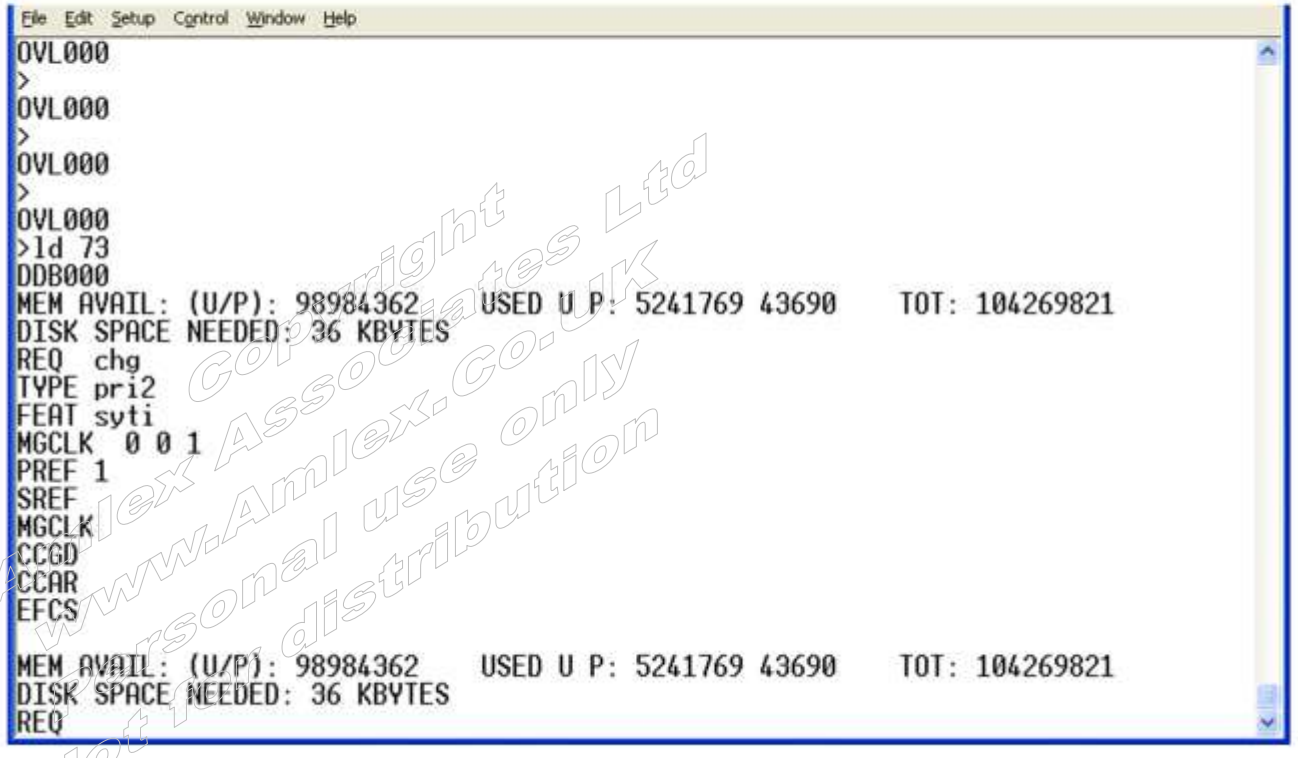
Copyright Amlex Associates Ltd

Adding a Clock Controller

The Clock Controller is added in LD 73 and is used to synchronise the transmissions.

The Clock Type is MGCLK and it should be noted that every Media Gateway with a PRI card in it will need a separate clock controller.

The PREF & SREF prompts are the Primary and Secondary References.



Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

298

Notes

_____

_____

_____

_____

Enabling the MSDL Card

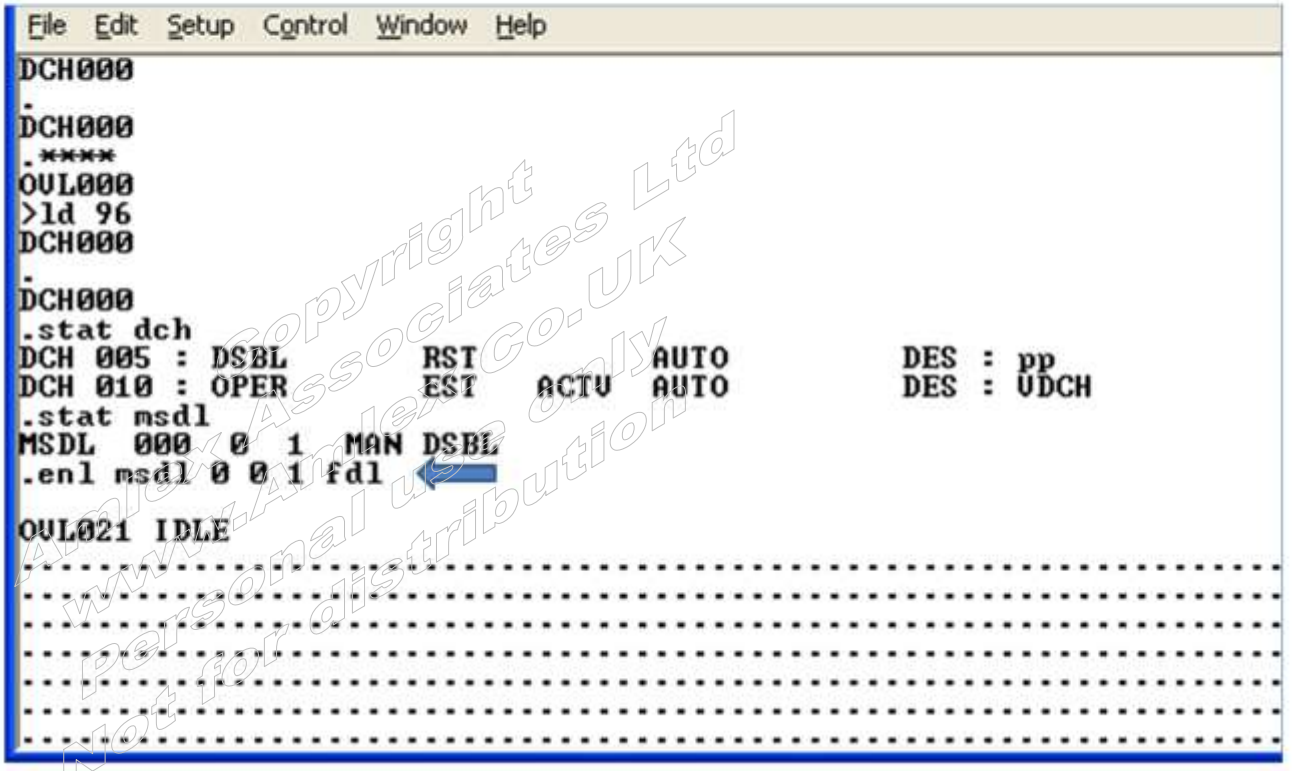
The MSDL D-Channel card now needs to be enabled and as this will be the first time its been used in this configuration we will also carry out a Force Download (FDL) at the same time.

>LD 96

.enl msdl (TN of card) fdl

As the download occurs you should see the “Dots” march across the screen as data is sent to the card. On completion you should get an OK message.

Use STAT MSDL <TN> to check that it is in service.



Amlex Copyright
www.Amlex Associates Ltd
personal use only
Not for distribution

299

Notes

_____

_____

_____

_____

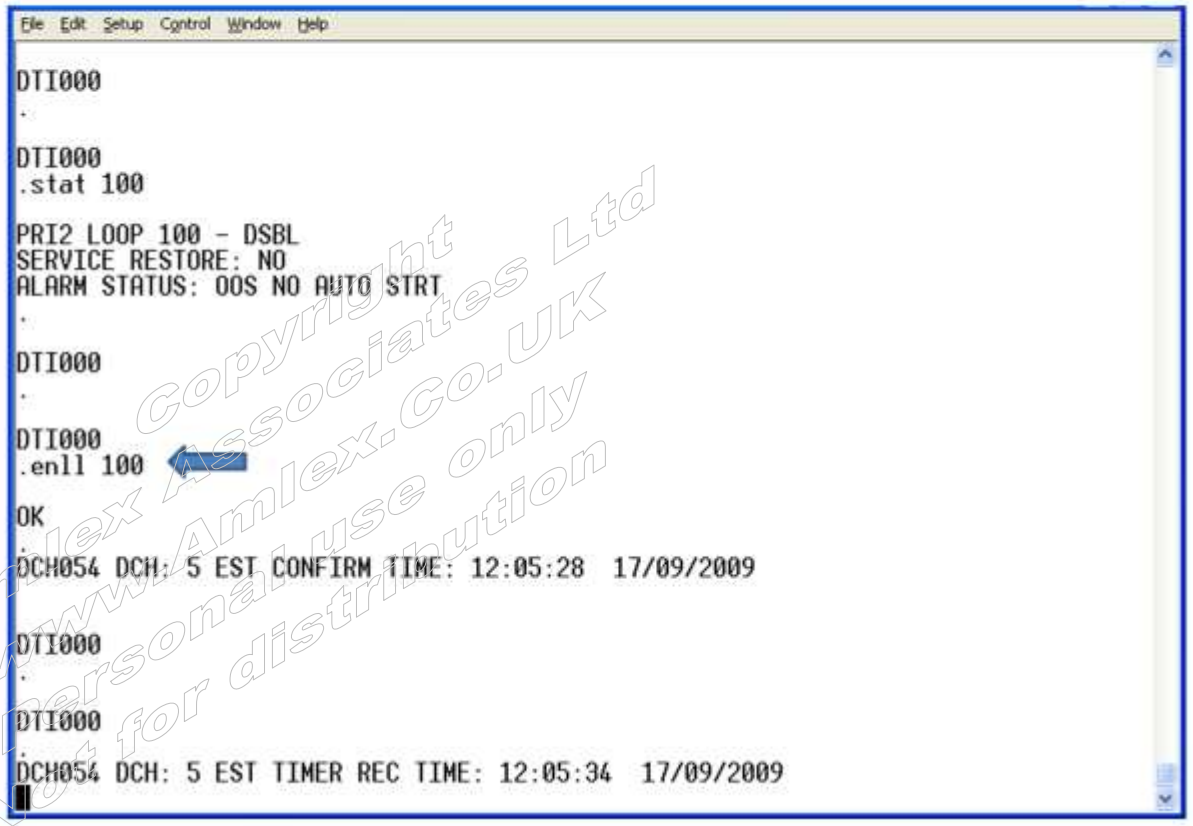
Copyright Amlex Associates Ltd

Enable PRI LOOP

Once the D-Channel card is enables we can try to establish the link.

In LD 60 we can use the **ENLL <Loop Number>** to bring the LOOP into service. This needs to be done on both systems i.e. both ends of the link before the service will correctly establish.

If necessary the LOOP can be disabled using the **DISL <Loop Number>** command and the counters listed **LCNT** and reset **RCNT** before re-enabling the LOOP to clear any issues.



Amlex Copyright
www.Amlex.Co.UK
Associates Ltd
Personal use only
Not for distribution

300

Notes

_____

_____

_____

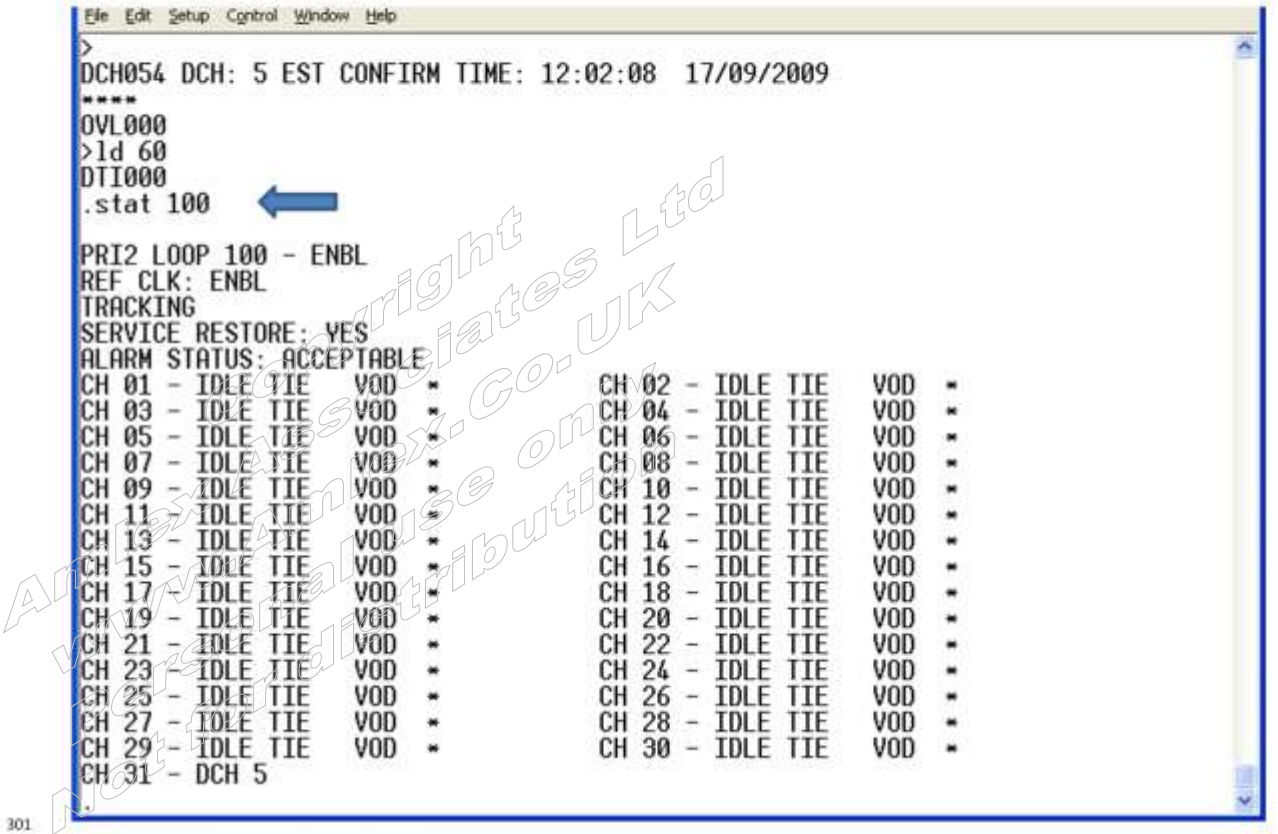
_____

Copyright Amlex Associates Ltd

STAT the LOOP

Once the card is enabled correctly you should see messages similar to those shown on the screenshot confirming the D-Channel is established and the PRI channels IDLE and available.

You will also note the ALARM STATUS: ACCEPTABLE message which highlights any issues. Further configuration of the Clock Controller may be necessary to avoid timing issues in this configuration.


File Edit Setup Control Window Help
>
DCH054 DCH: 5 EST CONFIRM TIME: 12:02:08 17/09/2009
****
OVL000
>ld 60
DTI000
.stat 100
PRI2 LOOP 100 - ENBL
REF CLK: ENBL
TRACKING
SERVICE RESTORE: YES
ALARM STATUS: ACCEPTABLE
CH 01 - IDLE TIE VOD * CH 02 - IDLE TIE VOD *
CH 03 - IDLE TIE VOD * CH 04 - IDLE TIE VOD *
CH 05 - IDLE TIE VOD * CH 06 - IDLE TIE VOD *
CH 07 - IDLE TIE VOD * CH 08 - IDLE TIE VOD *
CH 09 - IDLE TIE VOD * CH 10 - IDLE TIE VOD *
CH 11 - IDLE TIE VOD * CH 12 - IDLE TIE VOD *
CH 13 - IDLE TIE VOD * CH 14 - IDLE TIE VOD *
CH 15 - IDLE TIE VOD * CH 16 - IDLE TIE VOD *
CH 17 - IDLE TIE VOD * CH 18 - IDLE TIE VOD *
CH 19 - IDLE TIE VOD * CH 20 - IDLE TIE VOD *
CH 21 - IDLE TIE VOD * CH 22 - IDLE TIE VOD *
CH 23 - IDLE TIE VOD * CH 24 - IDLE TIE VOD *
CH 25 - IDLE TIE VOD * CH 26 - IDLE TIE VOD *
CH 27 - IDLE TIE VOD * CH 28 - IDLE TIE VOD *
CH 29 - IDLE TIE VOD * CH 30 - IDLE TIE VOD *
CH 31 - DCH 5
.
301

Amlex Associates Ltd Copyright www.amlex.co.uk Not to be used for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

25. NFS Deployment

The concept of the NFS (Network File System) install is to combine the three installation steps for a fully deployed Linux server into one operation.

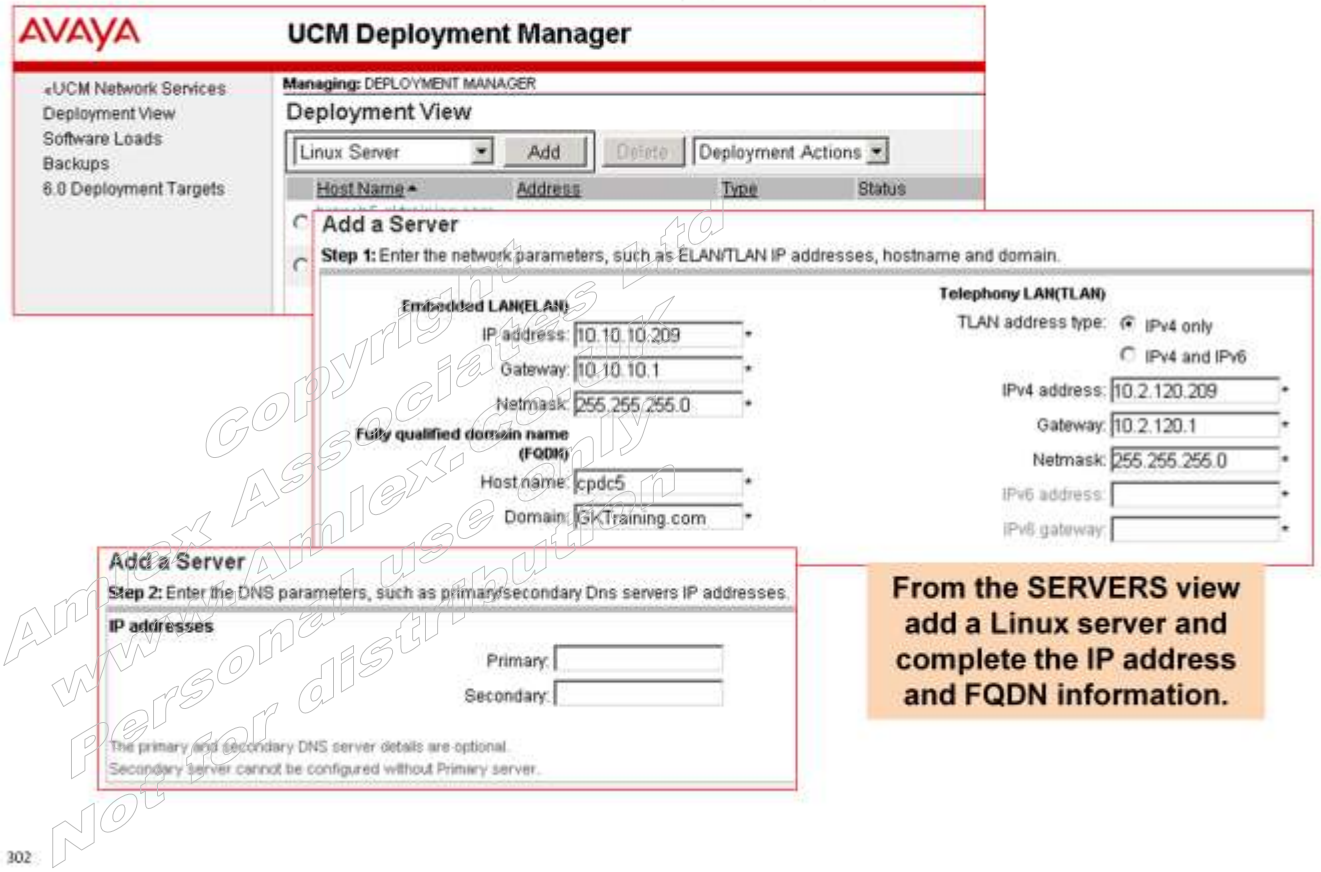
Without it the steps are

1. Install Linux Base
2. Security Configuration
3. Deploy Applications

With the NFS installation the Pre-Deployment stage sets up how the server will be configured right through to Application Deployment .

Firstly we must add the Linux Server itself so from **SERVERS** view we **ADD** a **LINUX SERVER** and we re prompted to complete the IP addresses and FQDN for the server.

Moving to the next screen we are prompted for the DNS settings for the server. Normally these would be completed but here we are leaving them blank.



Copyright Amlex Associates Ltd
www.Amlex.com
Personal use only
Not for distribution

Notes

_____

_____

_____

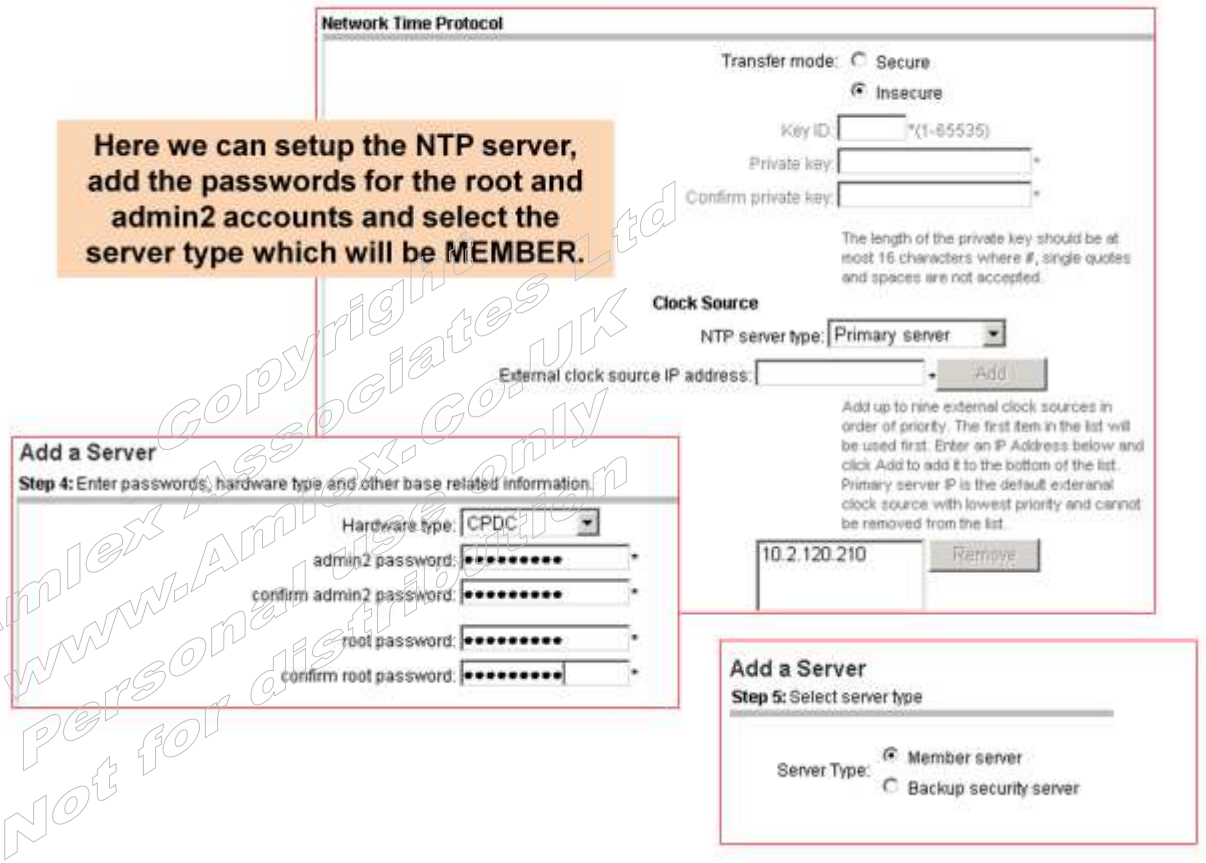
_____

As you can see here the system will prompt for the same information that would have been entered during a normal command line installation . (i.e. baseparamsconfig)

Here we can select the NTP server which is set to the System Manager by default. In addition we add the "**root**" and "**admin2**" account passwords.

The bottom screen asks for the server type which will be **MEMBER**.

Configure Linux Server


Here we can setup the NTP server, add the passwords for the root and admin2 accounts and select the server type which will be MEMBER.
Network Time Protocol
Transfer mode: Secure
Insecure
Key ID: *(1-65535)
Private key: *
Confirm private key: *
The length of the private key should be at most 16 characters where #, single quotes and spaces are not accepted.
Clock Source
NTP server type: Primary server
External clock source IP address: Add
Add up to nine external clock sources in order of priority. The first item in the list will be used first. Enter an IP Address below and click Add to add it to the bottom of the list. Primary server IP is the default external clock source with lowest priority and cannot be removed from the list.
10.2.120.210 Remove
Add a Server
Step 4: Enter passwords, hardware type and other base related information
Hardware type: CPDC
admin2 password: *
confirm admin2 password: *
root password: *
confirm root password: *
Add a Server
Step 5: Select server type
Server Type: Member server
Backup security server
303

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Configure Certificate

Finally we configure the server Certificate, firstly checking the Primary UCM Fingerprint.

Note that the Certificate information will be populated using the information from the System Manager so there may be some settings that will need to be changed such as the Country or Locality etc.

This will complete the Pre-Configuration of the Linux Server ready for the Applications to be selected.

Finally we need to complete the Certificate information.
The first step is to confirm the System Manager details and Fingerprint. Then the Certificate is completed and created.
Add a Server
Step 6: Verify primary security server fingerprint.
Address of the Primary security server : 10.2.128.210:443
Fully Qualified Domain Name (FQDN) of the Primary security server : smgr2.gktraining.com:443
The fingerprint of the primary security server is : 4c:27:2d:89:0c:7b:9e:53:be:89:3a:19:dc:3f:1c:96
Add a Server
Step 7: Enter certificate information.
Certificate Information
Friendly name: cpdc5.GKTraining.com
Bit length: 1024
Organization: Avaya
Organizational unit: Default Org Unit
Common name: cpdc5.GKTraining.com
Country/Region: UNITED KINGDOM
State/Province: Default State
City/Locality: Default City
NOTE:- The Certificate information is inherited from the System Manager but its important to check it, especially for Country etc. before saving.
304

Notes

_____

_____

_____

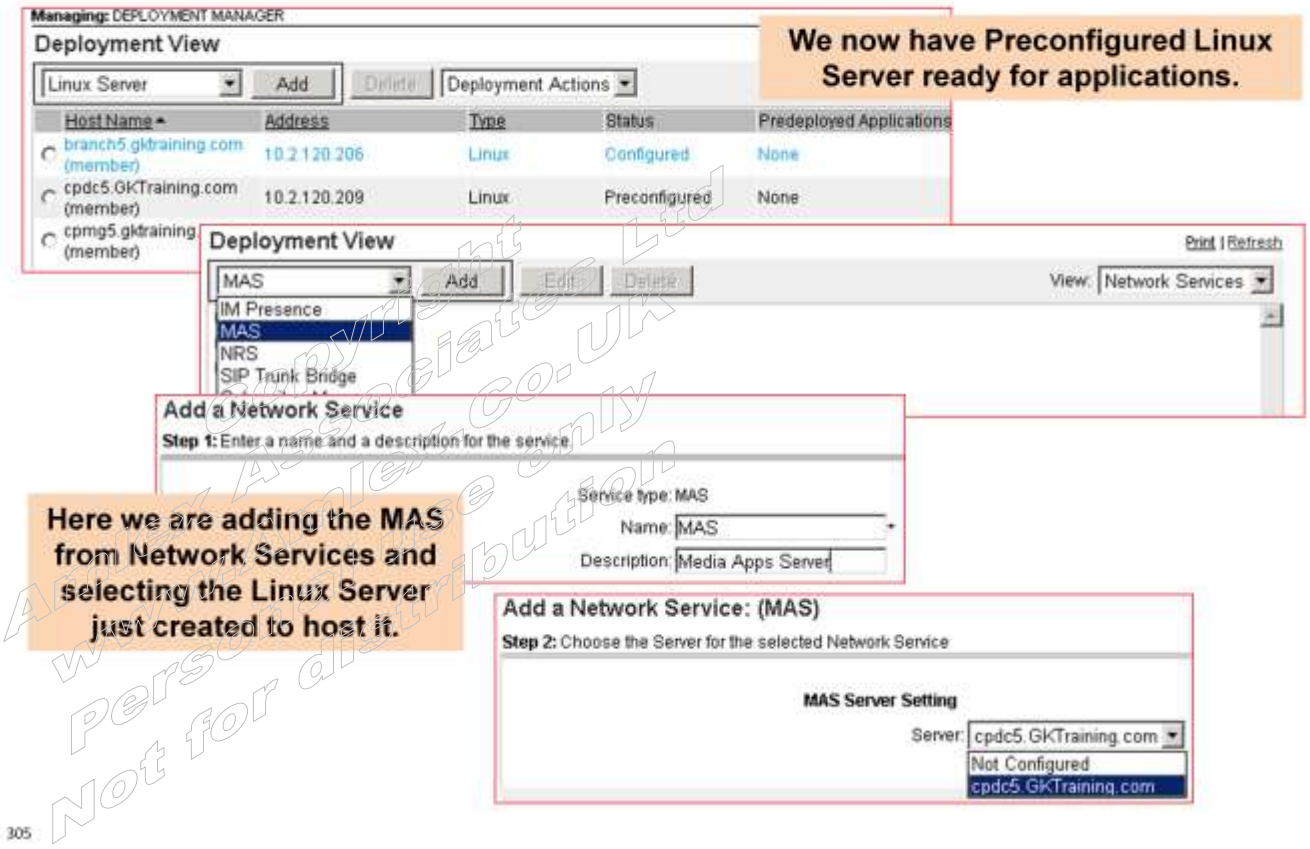
_____

Copyright Amlex Associates Ltd

Pre-Deploy MAS Server

Back at the Deployment View screen we can now see the Pre-Configured CPDC5 Linux sever. What we will do next is to add the Media Applications Server for deployment on the Linux server created.

From the **NETWORK SERVICES** view we select the MAS application, add a name for the server and then assign it to the Linux server cpdc5.GKTraining.com which we have Pre-Configured.



Copyright Amlex Associates Ltd
Personal use only
Not for distribution

Notes

_____

_____

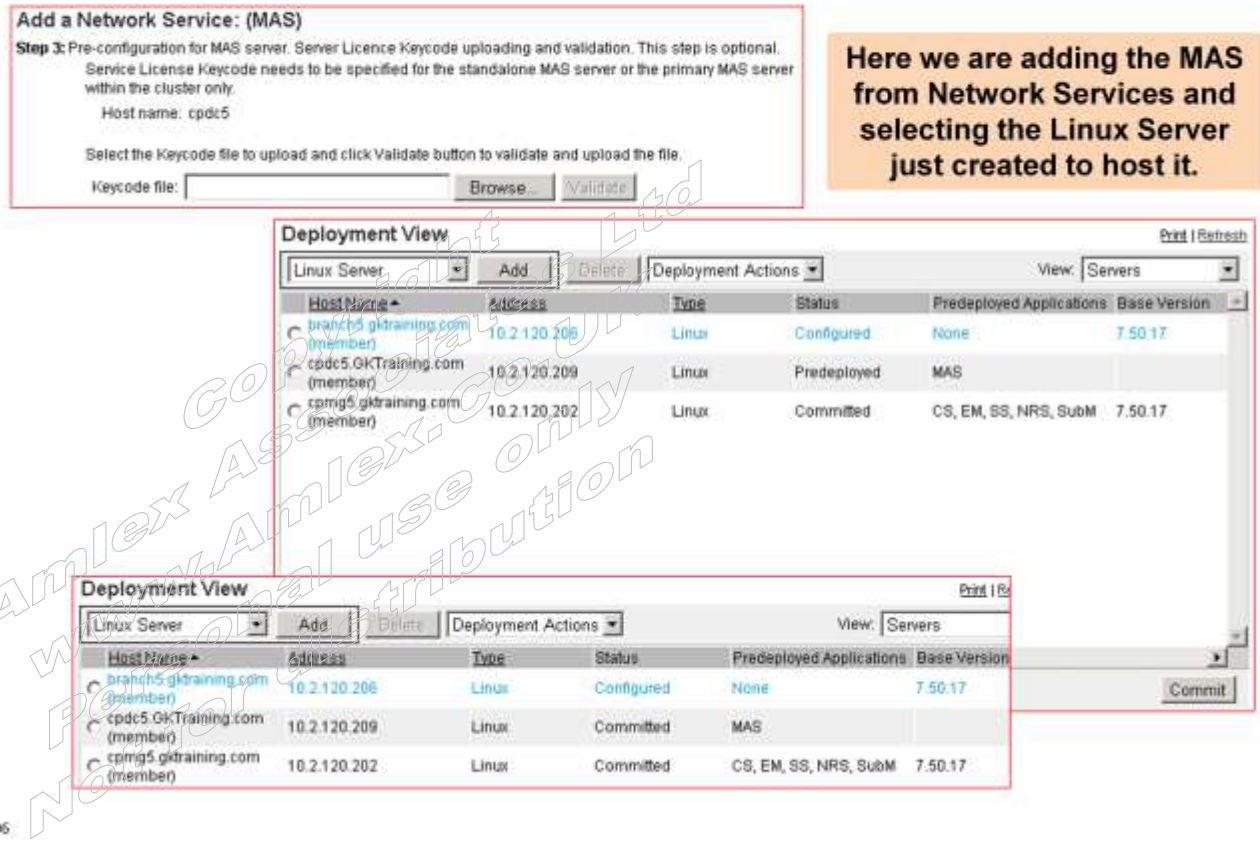
_____

_____

As you can see here you will be asked for a Keycode at this point as the MAS itself is licensed separately. However it is not necessary to add the license at this point as it can be added at a later stage. The License itself is locked to the MAC address of the server.

With the Application assigned now we can see the Server in the **SERVERS** list with MAS Predeployed . At this point we need to **COMMIT** the configuration ready for the installation.

Commit Deployment



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
No distribution

306

Notes

_____

_____

_____

_____

Install to Card

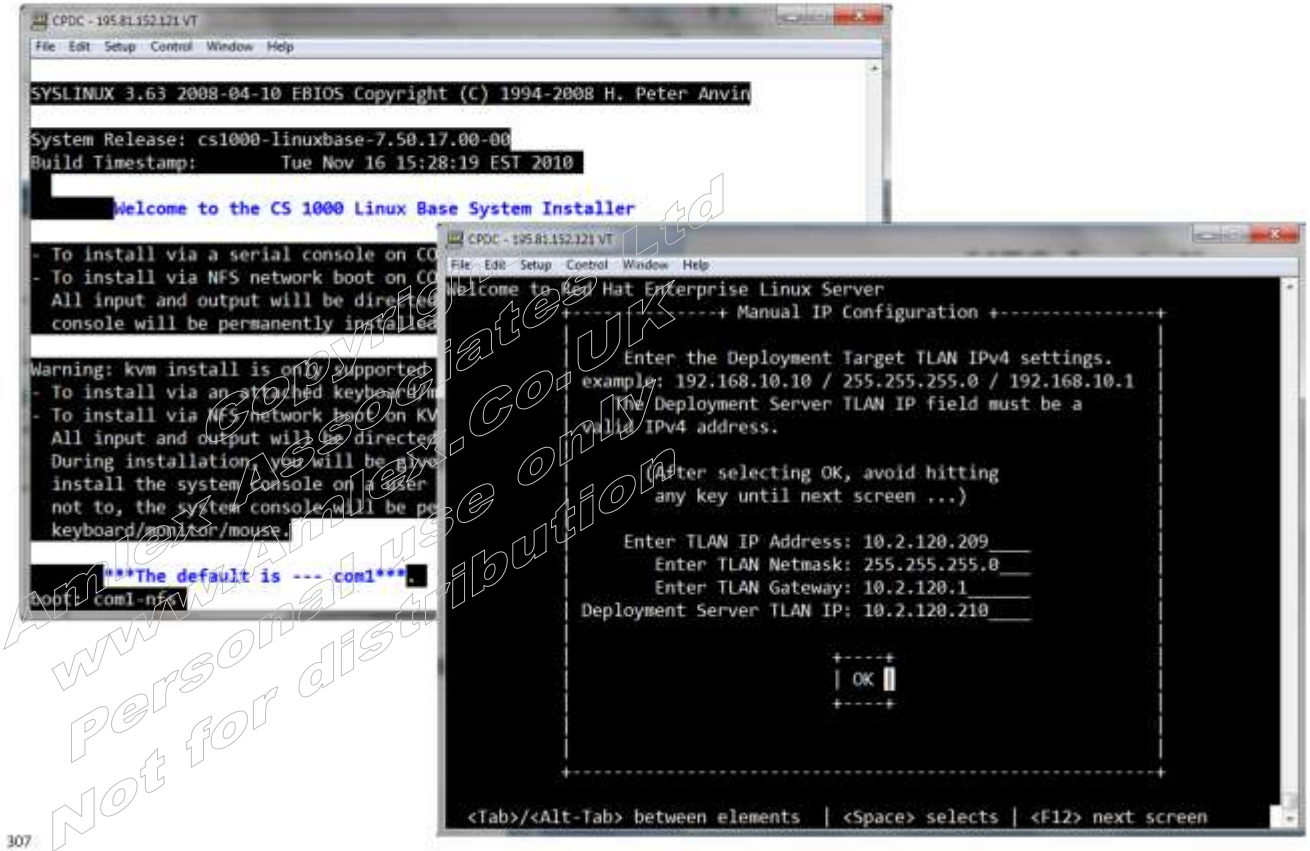
Now we move to the card to be installed. At boot up we will as before press the **F** key and select the USB stick as the boot device. However when the boot: option is displayed we now type :-

com1-nfs

To boot to the NFS option. This will display the screen far right prompting for the TLAN IP addresses for the card and the Deployment server which will be the System Manager itself.

Be careful entering the information on this screen. Use the TAB key to move from line to line and the OK button but use the SPACEBAR to click or select the OK itself.

This will begin the process of installation and deployment and the server can be left to process with no further input assuming there are no errors.


CPDC - 195.81.152.121 VT
File Edit Setup Control Window Help
SYSLINUX 3.63 2008-04-10 EBIOS Copyright (C) 1994-2008 H. Peter Anvin
System Release: cs1000-linuxbase-7.50.17.00-00
Build Timestamp: Tue Nov 16 15:28:19 EST 2010
Welcome to the CS 1000 Linux Base System Installer
- To install via a serial console on CO
- To install via NFS network boot on CO
All input and output will be direc
console will be permanently instal
Warning: kvm install is only supported
- To install via an attached keyboard/m
- To install via NFS network boot on KV
All input and output will be directed
During installation, you will be giv
install the system console on a user
not to, the system console will be p
keyboard/monitor/mouse.
The default is --- com1
boot: com1-nfs
CPDC - 195.81.152.121 VT
File Edit Setup Control Window Help
Welcome to Red Hat Enterprise Linux Server
Manual IP Configuration
Enter the Deployment Target TLAN IPv4 settings.
example: 192.168.10.10 / 255.255.255.0 / 192.168.10.1
KV Deployment Server TLAN IP field must be a
valid IPv4 address.
(After selecting OK, avoid hitting
any key until next screen ...)
Enter TLAN IP Address: 10.2.120.209
Enter TLAN Netmask: 255.255.255.0
Enter TLAN Gateway: 10.2.120.1
Deployment Server TLAN IP: 10.2.120.210
OK
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

307

Notes

_____

_____

_____

_____

26. Media Application Server

- Media Application Server
  - Replaces TDM Resources with IP Services
    - MIRAN
    - Conference & Tones
    - Music on Hold
  - Only Available on CPDC and COTS 2
  - Deployed the same as any system
    - Linux Base install
    - Deploy the Network Service
      - MAS
      - Can be deployed using NFS
  - Ensure install has completely finished before accessing the server
  - MAS is configured using its own separate "Element Manager"
    - Link created in Elements List
    - Install MS Silverlight for some screens to work correctly.

308

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

The Media Application Server is a new option with Release 7 of the CS1K suite. It offers the option of delivering traditionally TDM based services directly using IP e.g. Music on hold, conferencing announcements etc.

It is currently only supported on the COTS2 and CPDC platforms and requires a specific license linked to the MAC address of the device its installed on.

The deployment is similar to that of any existing Network Service such as the NRS or Subscriber Manager. It can also be installed using the NFS option from the Primary UCM, whereby Linux and the application are installed in one operation.

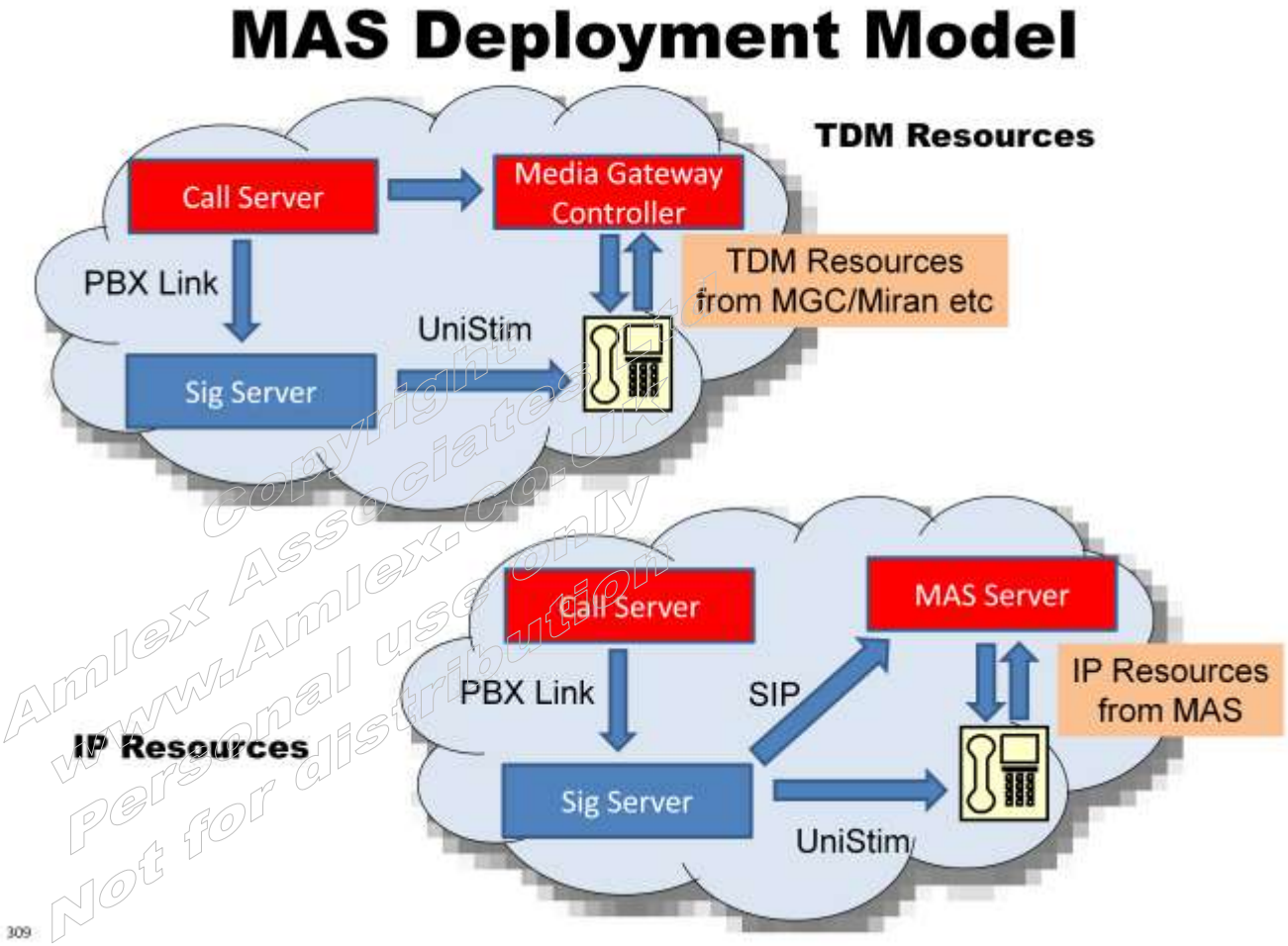
The MAS server has its own specific Element Manager and certain screens rely on MS Silverlight to perform correctly.

Notes

Here you can see the change in operation from a TDM only system whereby the Call server controls the resources which are predominantly housed within the Media gateway. Thus services such as conferencing are hosted on the conference packs on the MGC card and require Media Card channels to be used by IP sets.

In the IP/MAS scenario the resources are delivered on IP directly from the MAS server. The MAS is controlled using SIP via the Signalling server using a Media services Controller (MSC) . The services are then delivered directly to the IP set from the MAS eliminating the need for media card channels.

IP and TDM options are not mutually exclusive and we can support both on a system. The system will then select the most appropriate resource at the point a call is placed. The selection is based upon the call type IP/TDM and resource availability.



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

Notes

_____

_____

_____

_____

Configuring the MAS

Once the MAS server has been installed it needs to be licensed and configured for use. The license can be installed during installation but this is not mandatory and allows for card changes !

The following example shows its use as single server linked to a single call server. Note that the MAS can be used as a central resource for several systems controlled by SIP and accessed using either the NRS or Session Manager. It can also be scaled up to support very large installations by clustering MAS servers together.

In the screens here we are selecting the QUICK SETUP option and then the GENERAL SETTINGS to start the license process.

AVAYA
Avaya Media Server
Network
System Status
Element Status
Cluster Status
Alarms
Logs
Monitoring
Applications
Operational State
Signaling Translations
Custom Applications
Packaged Applications
Cluster Configuration
Server Designation
Replication Settings
Load Balancing
Advanced Settings
System Configuration
Quick Setup
Server Profile
Network Settings
Signaling Protocols
Media Processing
Application Interpreters
Monitoring Settings
Session Detail Records
Logging Settings
Debug Tracing
Engineering Parameters
Home » System Configuration » Quick Setup
Quick Setup
Server Role
To designate the role of this server within a cluster, click here.
Licensing
To configure licensing keys, configure and manage the license server, click here.
Avaya Media Server
Home » Licensing
Licensing
These tasks allow administrators to add or replace the license keys as well as to configure and manage the license server.
General Settings
This task allows administrators to enable the license server or nodal licensing. Administrators may also add or replace the license keys.
Monitoring
This task allows administrators to monitor license usage.
Server Status
This task allows administrators to manage the license server as well as display the status and operational mode.
Utilization Threshold
This task allows administrators to edit the license utilization threshold (in percentage).
Advanced Settings
This task allows administrators to manually configure the license server, which will override the Cluster Configuration settings. Administrators
license server.

Amlex Associates Ltd www.Amlexcd.co.uk Copyright Personal use only Not for distribution

310

Notes

_____

_____

_____

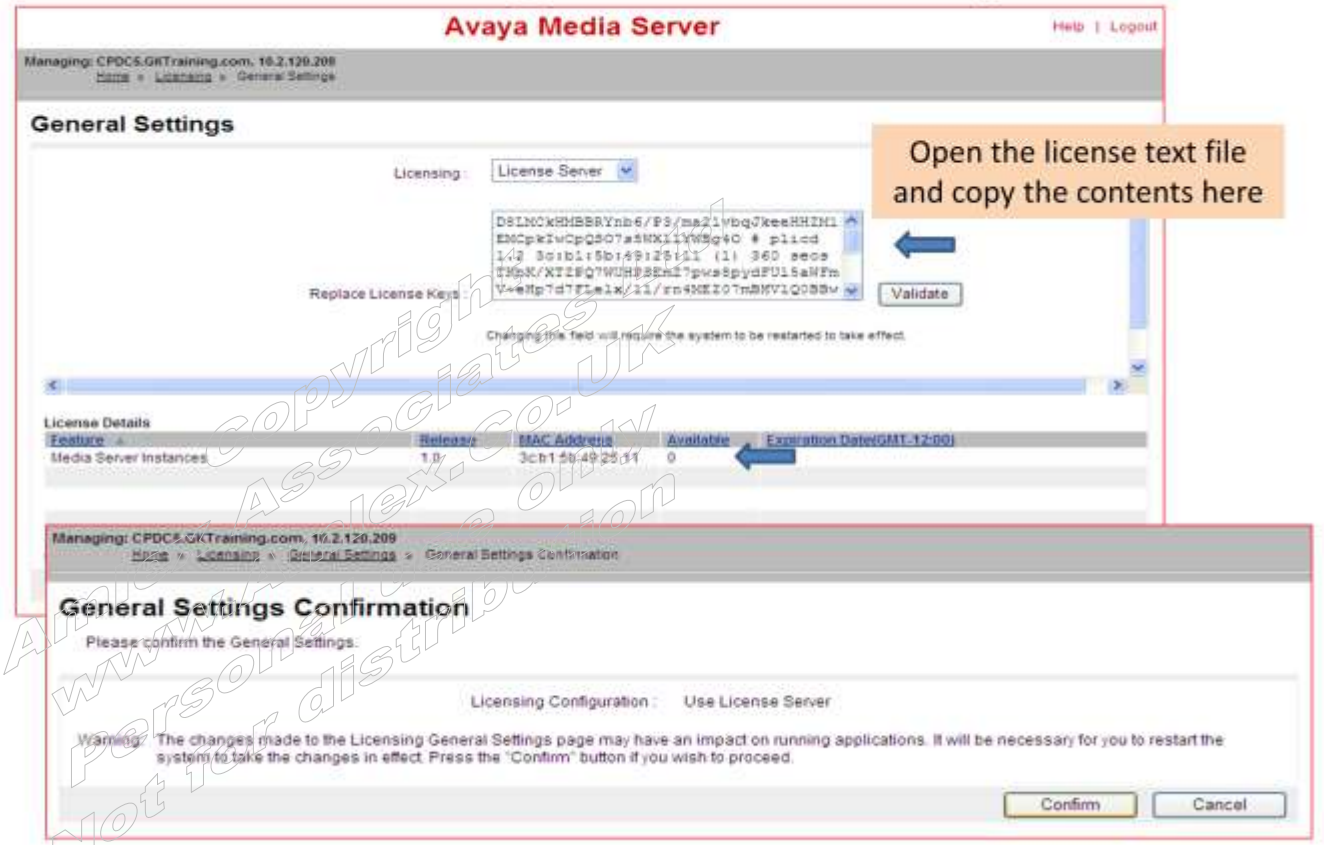
_____

Adding License Key

As you can see on the General Settings page we are prompted for the license. There are several different License options but in our example we are using the LICENSE SERVER and will merely paste in the appropriate keycode information.

When you click the VALIDATE button this will be checked and the license information shown in the lower part of the screen (Second Arrow).

On saving the information you will be asked to confirm the changes and advised that the system may need to be restarted to accept the changes. Just Click the CONFIRM Button, there is no need to restart or reboot the server at this point.


Avaya Media Server
Help | Logout
Managing: CPDC5.GKTraining.com, 10.2.120.209
Home » Licensing » General Settings
General Settings
Licensing : License Server
Open the license text file and copy the contents here
Replace License Key :
Validate
Changing this field will require the system to be restarted to take effect.
License Details
Feature
Release
MAC Address
Available
Expiration Date(GMT-12:00)
Media Server Instances
1.0
0
Managing: CPDC5.GKTraining.com, 10.2.120.209
Home » Licensing » General Settings » General Settings Confirmation
General Settings Confirmation
Please confirm the General Settings.
Licensing Configuration : Use License Server
Warning: The changes made to the Licensing General Settings page may have an impact on running applications. It will be necessary for you to restart the system to take the changes in effect. Press the "Confirm" button if you wish to proceed.
Confirm
Cancel

311

Notes

_____

_____

_____

_____

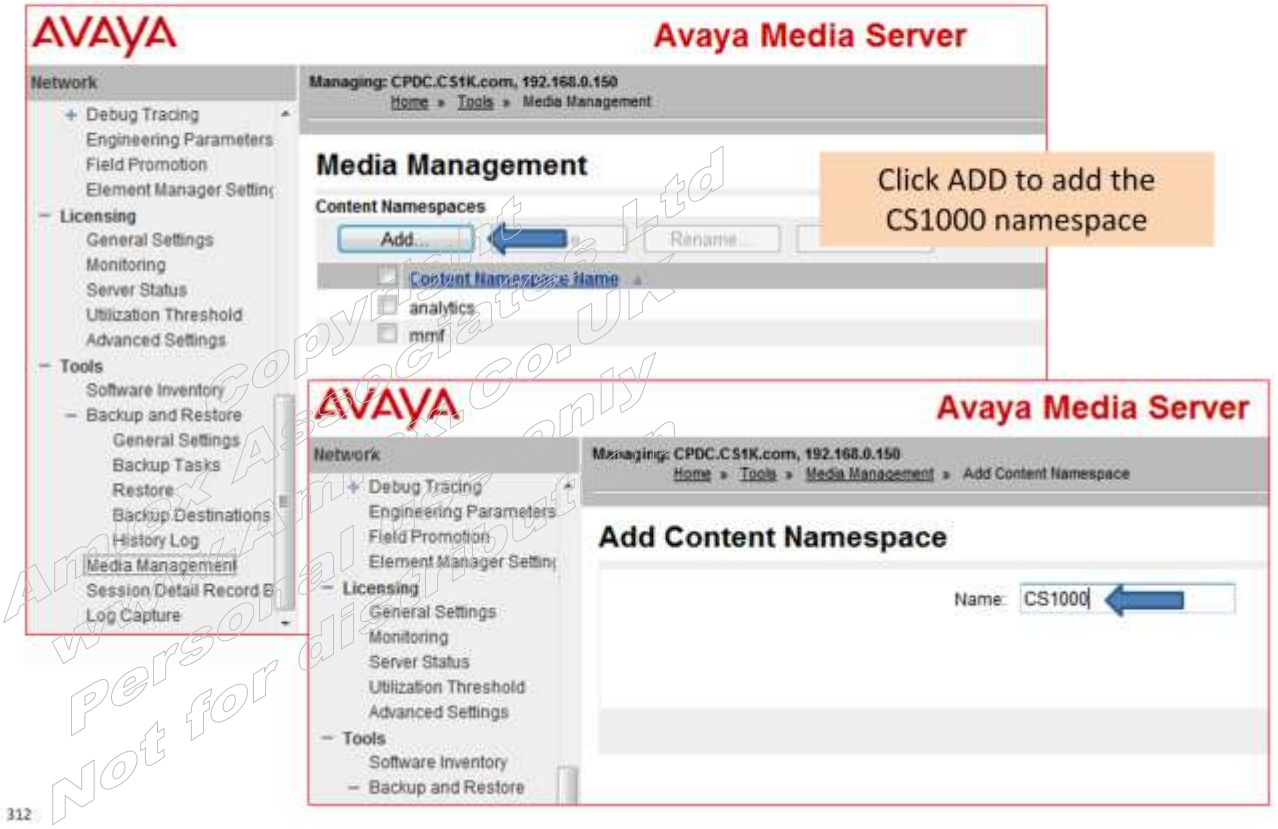
Copyright Amlex Associates Ltd

Add Content Namespace

Once the server is Licensed you can proceed to add the content that will be used. Before this can be done we need to add the Content Namespace.

It is critical to get this correct as the system will use this to access the files for Music and announcements etc.

Firstly we need to add a CS1000 space which the other entities will sit beneath. Using the ADD button you simply add the name and save it.



312

Notes

_____

_____

_____

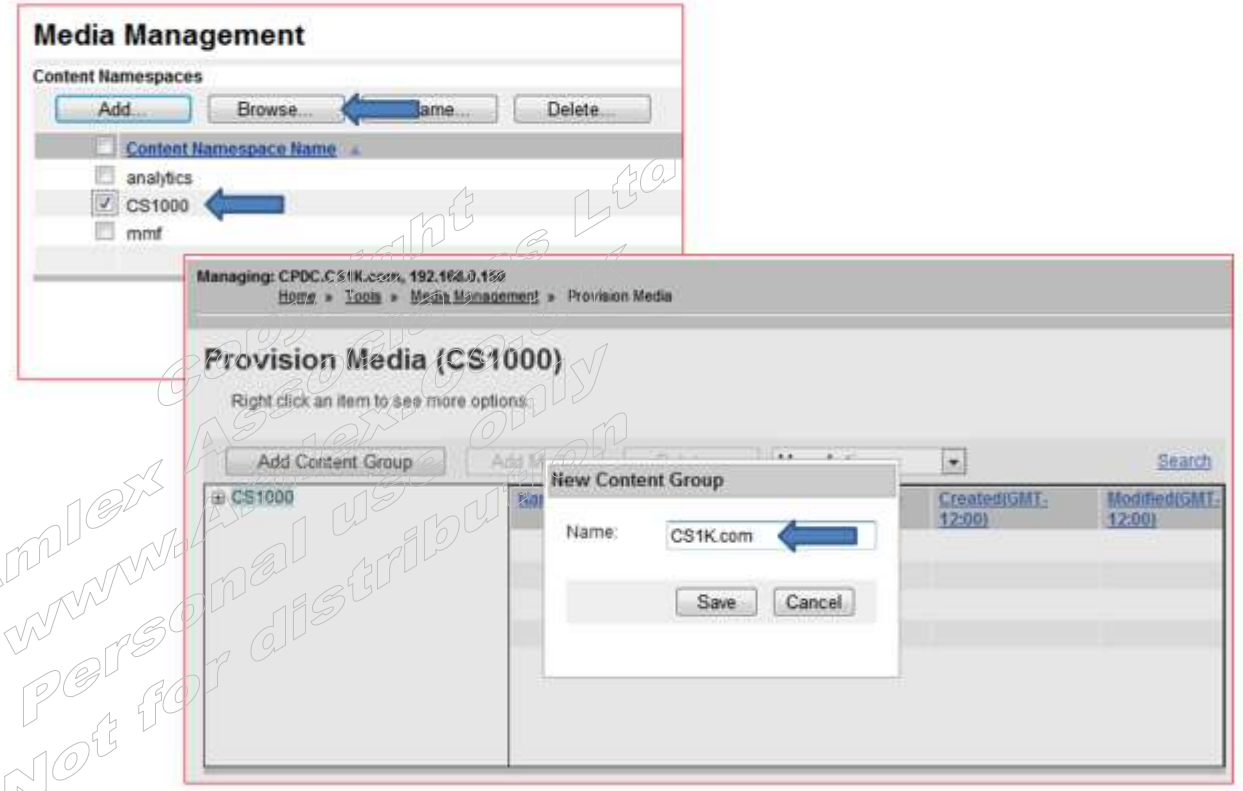
_____

Amlex Copyright Associates Ltd www.amlex.co.uk Personal use only Not for distribution

Add Content Group

With the Namespace created we can now add the Content Group below it. The first thing to add is the **SIP Domain** name we are using.

In this instance we have CS1K.com but this needs to be matched to the SIP domain setup on the CS1K system you are connecting to.



Notes

_____

_____

_____

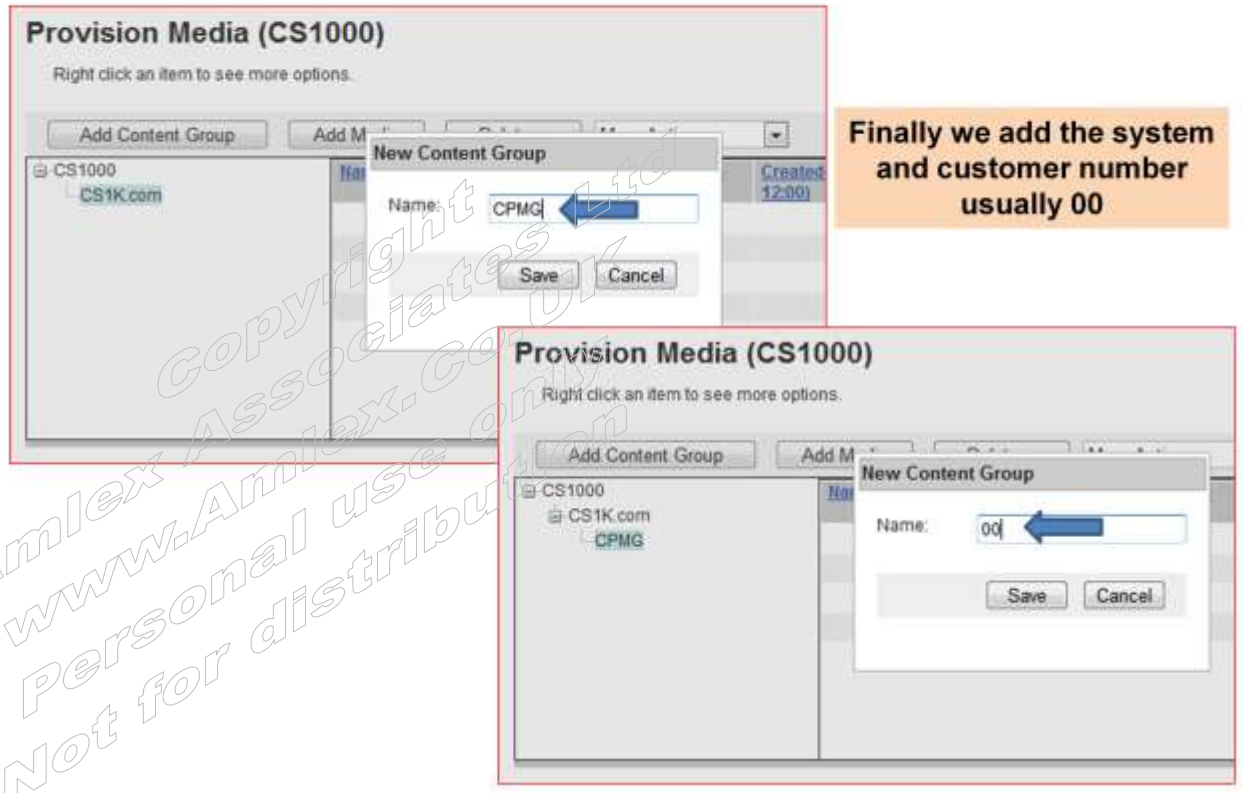
_____

Copyright Amlex Associates Ltd

Add System and Customer

Next we are adding the **system** and **customer number** as further sub directories. This is the path that the system will use to deliver the content so it must be correct.

If you have configured it incorrectly you can rename the folders at a later stage, there is no need to delete them and add them again.



Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

314

Notes

_____

_____

_____

_____

Add Media File

Here we are adding he Music on Hold resource inside the 00 (Customer) location.

The file is in a WAV format but when uploaded we select the tick box to remove the extension.

Naming is critical so make sure the name used is the same as the Music on Hold trunk number created on the system and it needs a 3 digit number as part of the name. This is the music route number, and if you have used say 20 you will need to add the leading zeros to ensure it is identified correctly. i.e. :-
For Music Route 20 the filename will be “mus020”.

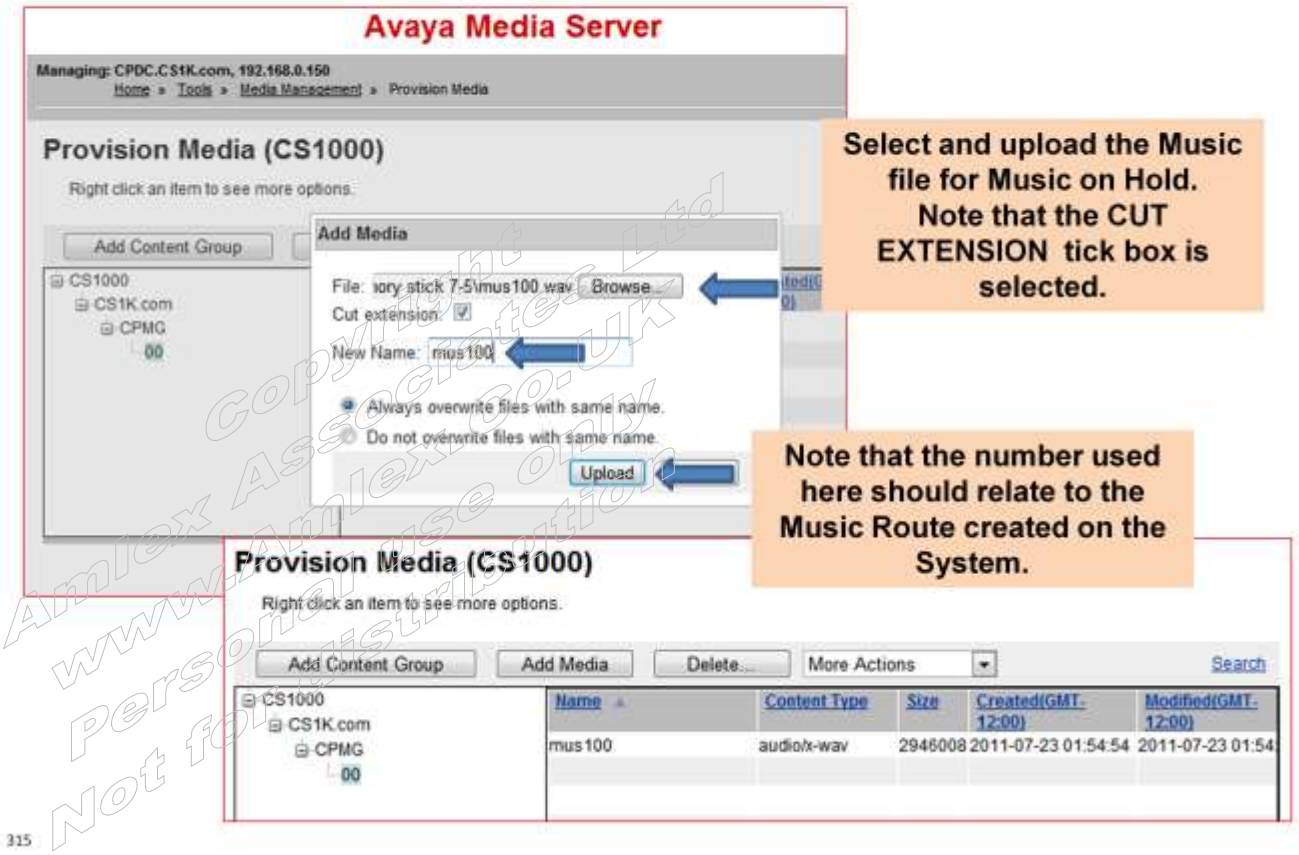
The Music Format should be:-

Audio Format PCM

Sample Rate 8.00kHz

Audio Sample Size 16Bit

Channels Mono



Amlex Associates Ltd www.Amlex.co.uk Copyright Personal use only Not for distribution

Notes

_____

_____

_____

_____

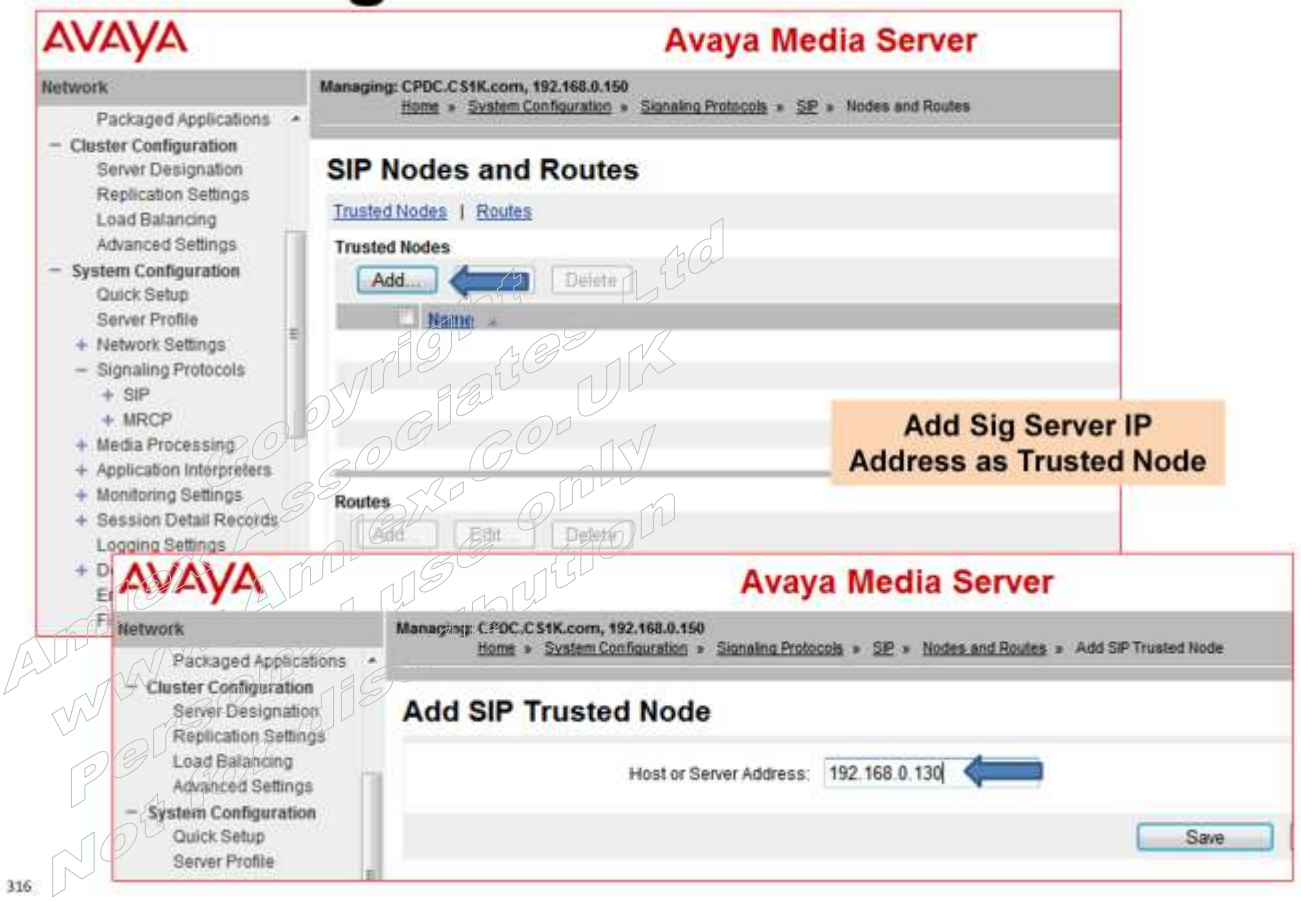
Copyright Amlex Associates Ltd

Configure the Trusted Node

The MAS is controlled by the MSC and therefore there needs to be a Trust between the two devices to allow communication.

To do this we select the SYSTEM CONFIGURATION/SIGNALLING PROTOCOLS/SIP page. We then add the IP address of the Signalling Server that will host the controlling MSC.

That is the basic configuration for the MAS itself.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Add MSC to IP Node in EM

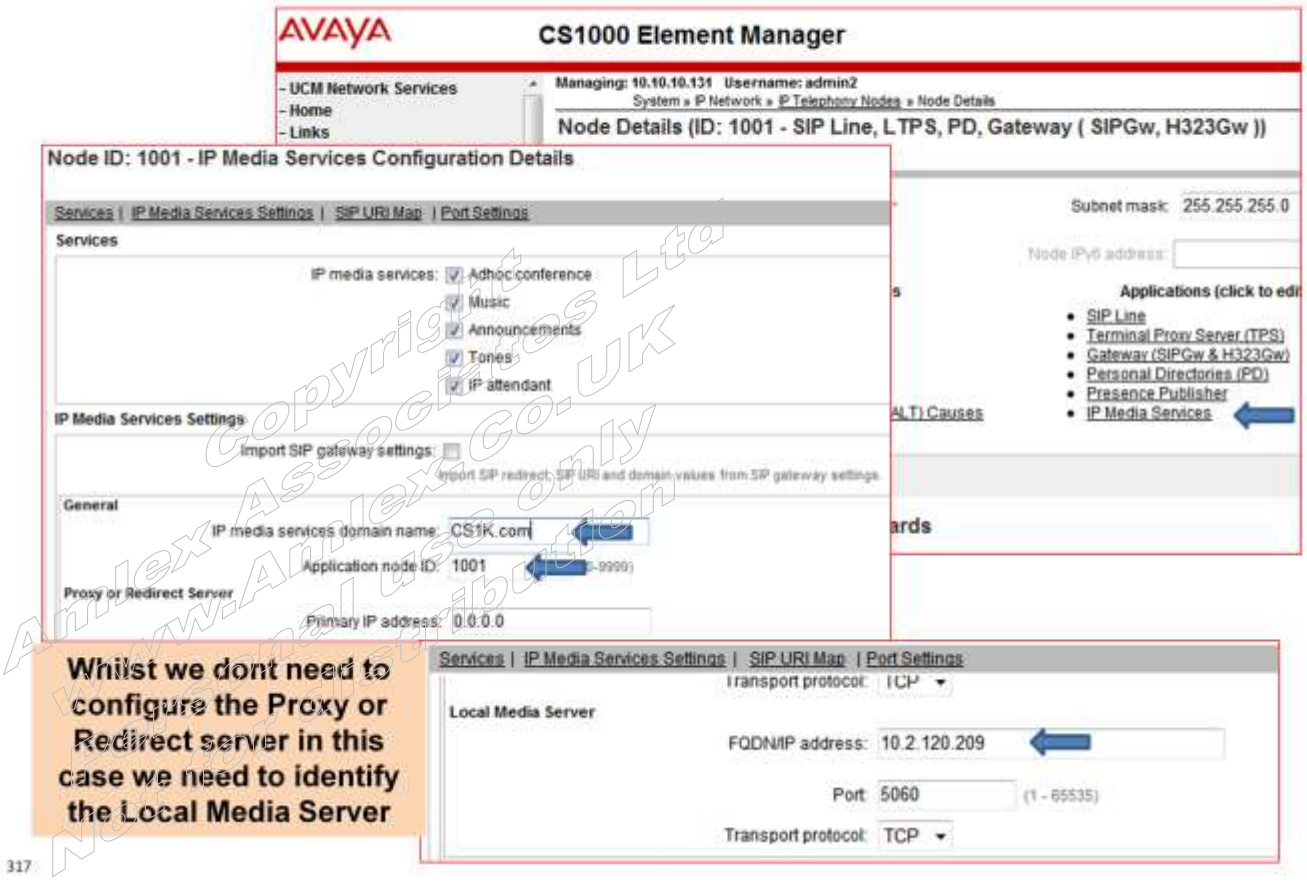
Returning to the System we will be linking the MAS to we first need to configure the MSC in the IP telephony Node.

As you can see here we have edited the IP Node and selected the option IP MEDIA SERVICES.

In the lower screen we have selected all of the services we want to use. Under the GENERAL area we have also included the SIP Domain name and the IP Node number.

In this example as the MAS is only associated with one server the PROXY or REDIRCT SERVER address has been left as 0.0.0.0. If the MAS were to be shared amongst several systems we would include the Session Manager or NRS address so it could determine the correct route o deliver services.

However we do need to identify the Local Media Server and this is shown in the lower screenshot.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
Managing: 10.10.10.131 Username: admin2
System » IP Network » IP Telephony Nodes » Node Details
Node Details (ID: 1001 - SIP Line, LTPS, PD, Gateway (SIPGw, H323Gw))
Node ID: 1001 - IP Media Services Configuration Details
Services | IP Media Services Settings | SIP URI Map | Port Settings
Services
IP media services: Adhoc conference
Music
Announcements
Tones
IP attendant
IP Media Services Settings
Import SIP gateway settings:
General
IP media services domain name: CS1K.com
Application node ID: 1001
Proxy or Redirect Server
Primary IP address: 0.0.0.0
Subnet mask: 255.255.255.0
Applications (click to edi
SIP Line
Terminal Proxy Server (TPS)
Gateway (SIPGw & H323Gw)
Personal Directories (PD)
Presence Publisher
IP Media Services
Whilst we dont need to configure the Proxy or Redirect server in this case we need to identify the Local Media Server
Services | IP Media Services Settings | SIP URI Map | Port Settings
Transport protocol: TCP
Local Media Server
FQDN/IP address: 10.2.120.209
Port: 5060 (1 - 65535)
Transport protocol: TCP
317

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

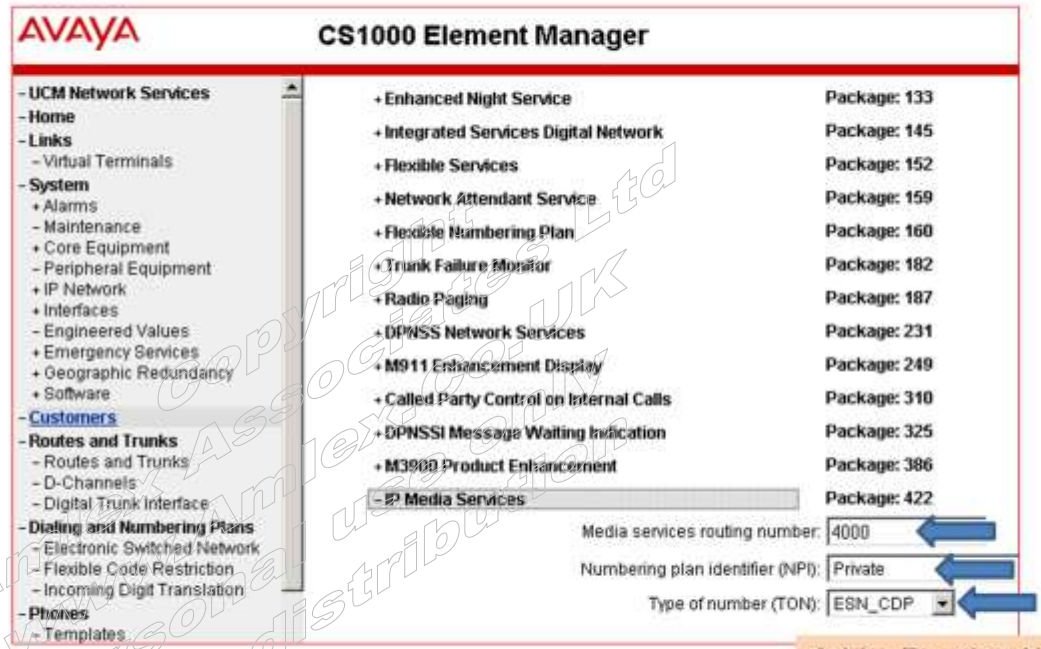
Enable Media Services Routing

Once the IP node has been completed and synchronised we can move on to add the Media service routes.

Firstly we must enable them in the Feature packages on the system and add a MEDIA SERVICES ROUTING NUMBER as shown here.

The NPI is Private
The TON is ESN_CDP

For a Local Server the MSRN is not used but for MAS Routing this is used to direct the calls to the MAS.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
+ Enhanced Night Service Package: 133
+ Integrated Services Digital Network Package: 145
+ Flexible Services Package: 152
+ Network Attendant Service Package: 159
+ Flexible Numbering Plan Package: 160
+ Trunk Failure Monitor Package: 182
+ Radio Paging Package: 187
+ DPNSS Network Services Package: 231
+ M911 Enhancement Display Package: 249
+ Called Party Control on Internal Calls Package: 310
+ DPNSSI Message Waiting Indication Package: 325
+ M3900 Product Enhancement Package: 386
- IP Media Services Package: 422
Media services routing number: 4000
Numbering plan identifier (NPI): Private
Type of number (TON): ESN_CDP
Add a Routing Number as shown to identify the IP Media Services.
318

Copyright Amlex Associates Ltd
Amlex Associates Ltd
Personal use only
Not for distribution

Notes

_____

_____

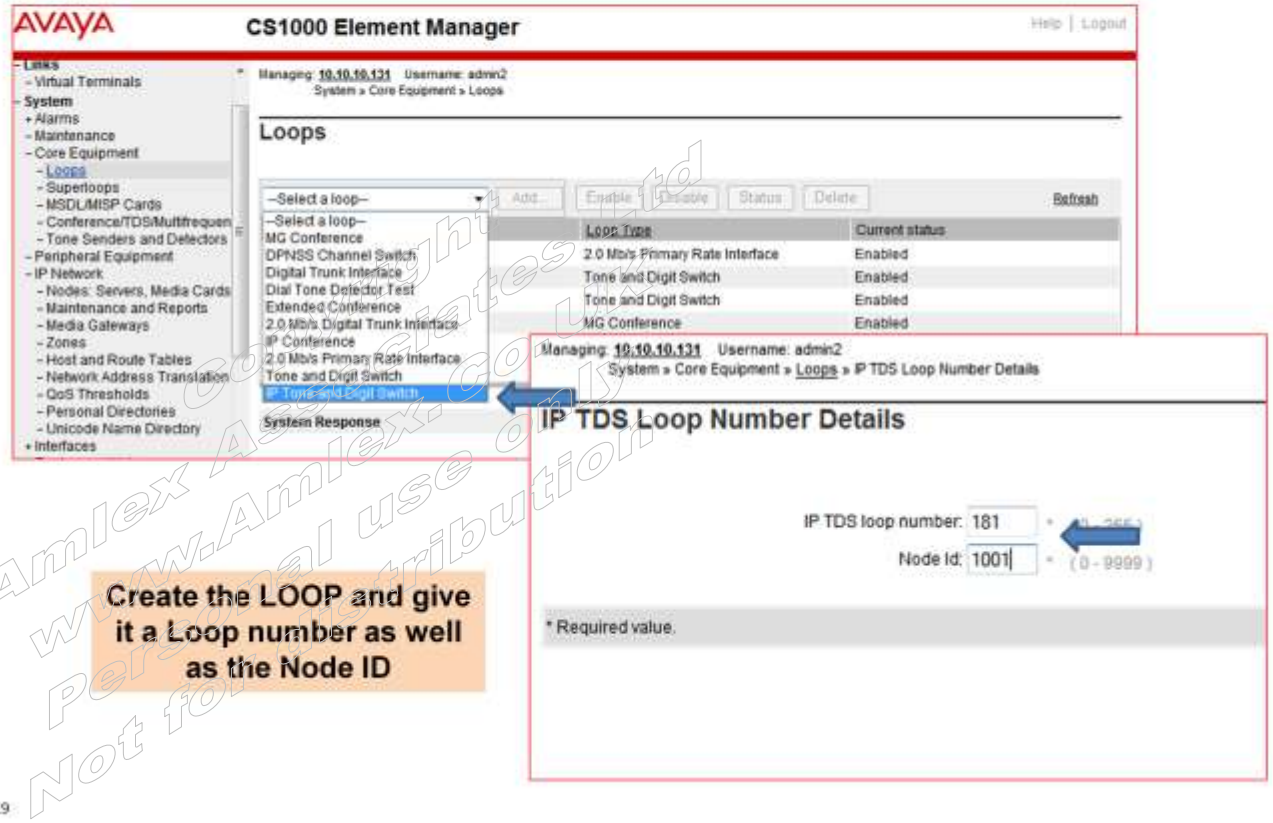
_____

_____

Adding Tone Loops

The MAS can replace all of the TDS & Conf resources we have or just augment them.

Here we are adding the IP TONES AND DIGIT SWITCH. Note that it will still need a LOOP number to identify it to the system but in addition e need to add the Node ID for the signalling server that is controlling the MAS (i.e. MSC)



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

319

Notes

_____

_____

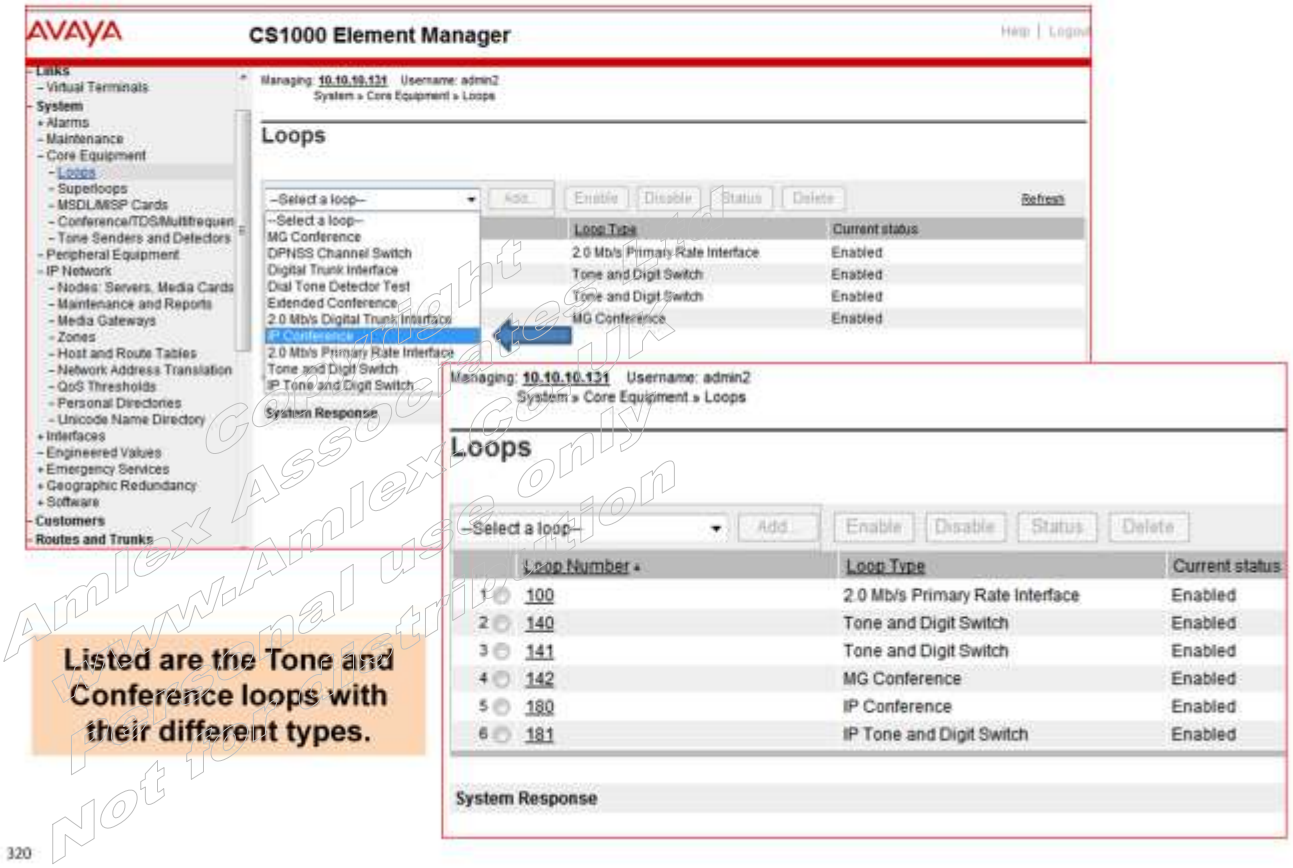
_____

_____

Copyright Amlex Associates Ltd

Adding Conference Loops

Add the IP Conference loops in a similar fashion.



Notes

_____

_____

_____

_____

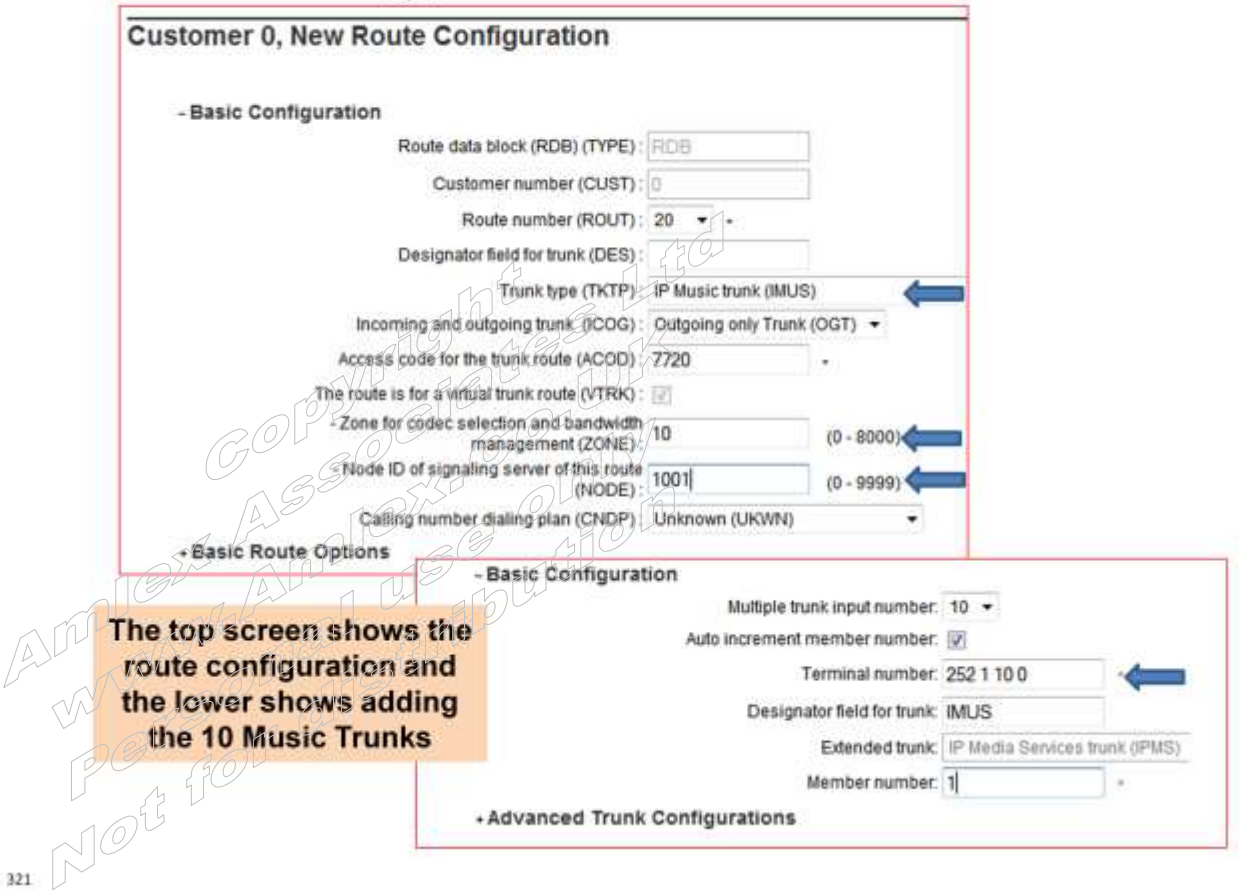
Copyright Amlex Associates Ltd

Configure IP Music Route

The Music Route is added in the normal fashion but note that the type is now IMUS IP Music Trunk.

In addition we need to add information such as a Bandwidth Zone and the Node ID. Also we need to assign a Virtual TN to each trunk as they are effectively Virtual Trunks.

Her we have created 10 Music Trunks starting at VTN 252 1 10 0.


Customer 0, New Route Configuration
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 0
Route number (ROUT) : 20
Designator field for trunk (DES) :
Trunk type (TKTP) : IP Music trunk (IMUS)
Incoming and outgoing trunk (ICOG) : Outgoing only Trunk (OGT)
Access code for the trunk route (ACOD) : 7720
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) : 10 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 1001 (0 - 9999)
Calling number dialing plan (CNDP) : Unknown (UKWN)
+ Basic Route Options
- Basic Configuration
Multiple trunk input number: 10
Auto increment member number:
Terminal number: 252 1 10 0
Designator field for trunk: IMUS
Extended trunk: IP Media Services trunk (IPMS)
Member number: 1
+ Advanced Trunk Configurations
The top screen shows the route configuration and the lower shows adding the 10 Music Trunks
321

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Monitor MAS Activity

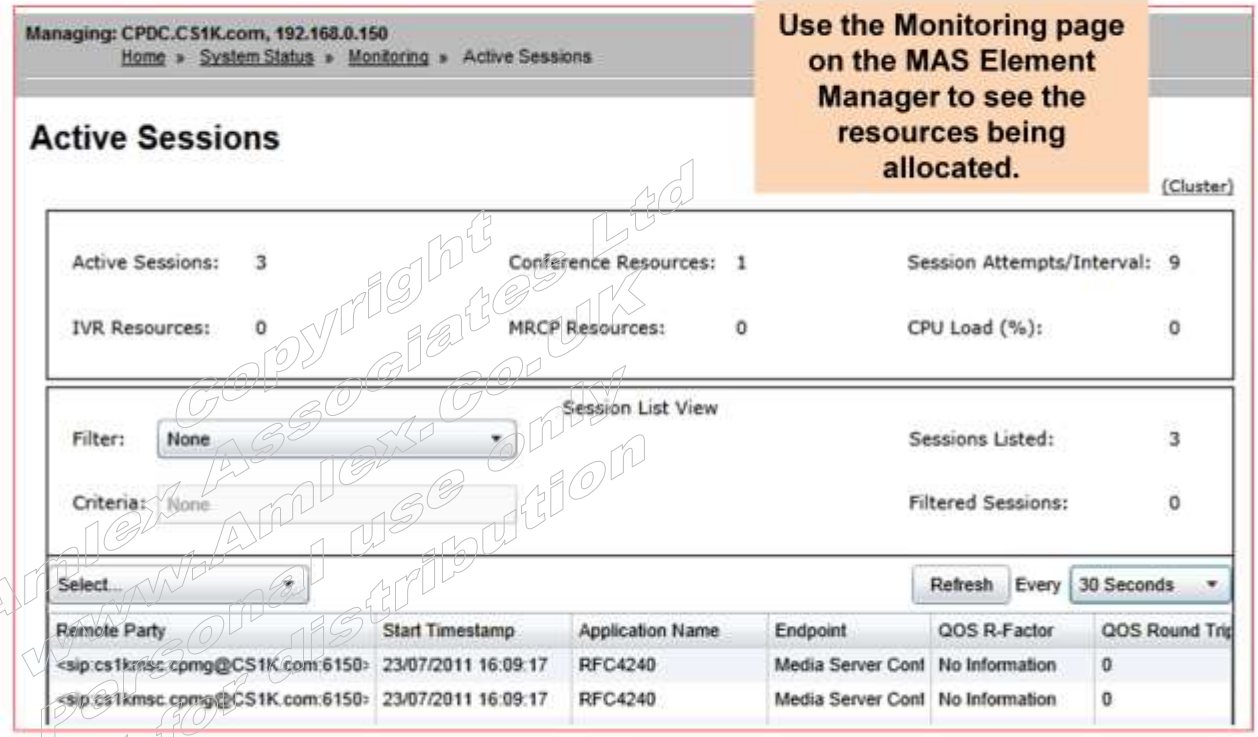
Assuming we've got everything correctly configured we can now edit the IP sets so that the following options are set :-

MRT Music Route Number
Should point to Music Route created

SBM Set Based Music
Should be set to ALLOWED

Putting a call on hold should now give them the Music directly from the MAS server.

Also try setting up a conference call and you should see a result similar to that shown with 3 or more active sessions and 1 conference resource in use. The display is dynamic and should update as you drop the call.



322

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

To enable the sharing of a MAS resource we need to use the Session Manager (or NRS) to redirect requests from the Call Servers to the MAS itself.

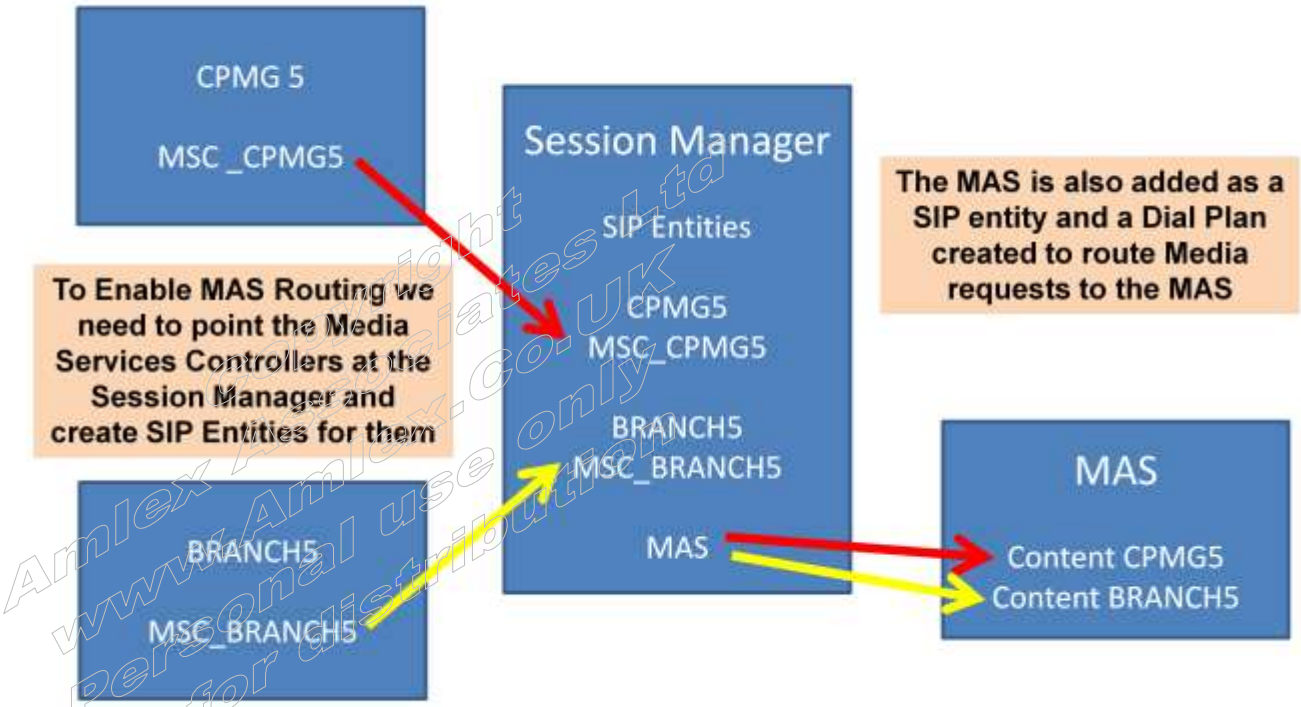
This is a simple diagram to illustrate what happens to a Media request from a call server to a shared MAS.

Firstly the Media Services Controller within the IP Telephony node of the Call Server is configured to point to the Session Manager and has a corresponding SIP Entity configured on the Session Manager. Thus any request generated using the Media Services Routing Number is passed to the Session Manager for Routing .

The MAS is also configured as a SIP Entity on the Session Manager and will receive and pass on to the MAS the Media request.

On the MAS itself, the actual Media is stored specifically for different Call Servers. The request is fulfilled using the appropriate media back to the requesting Call Server

MAS Routing



Amlex Associates ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

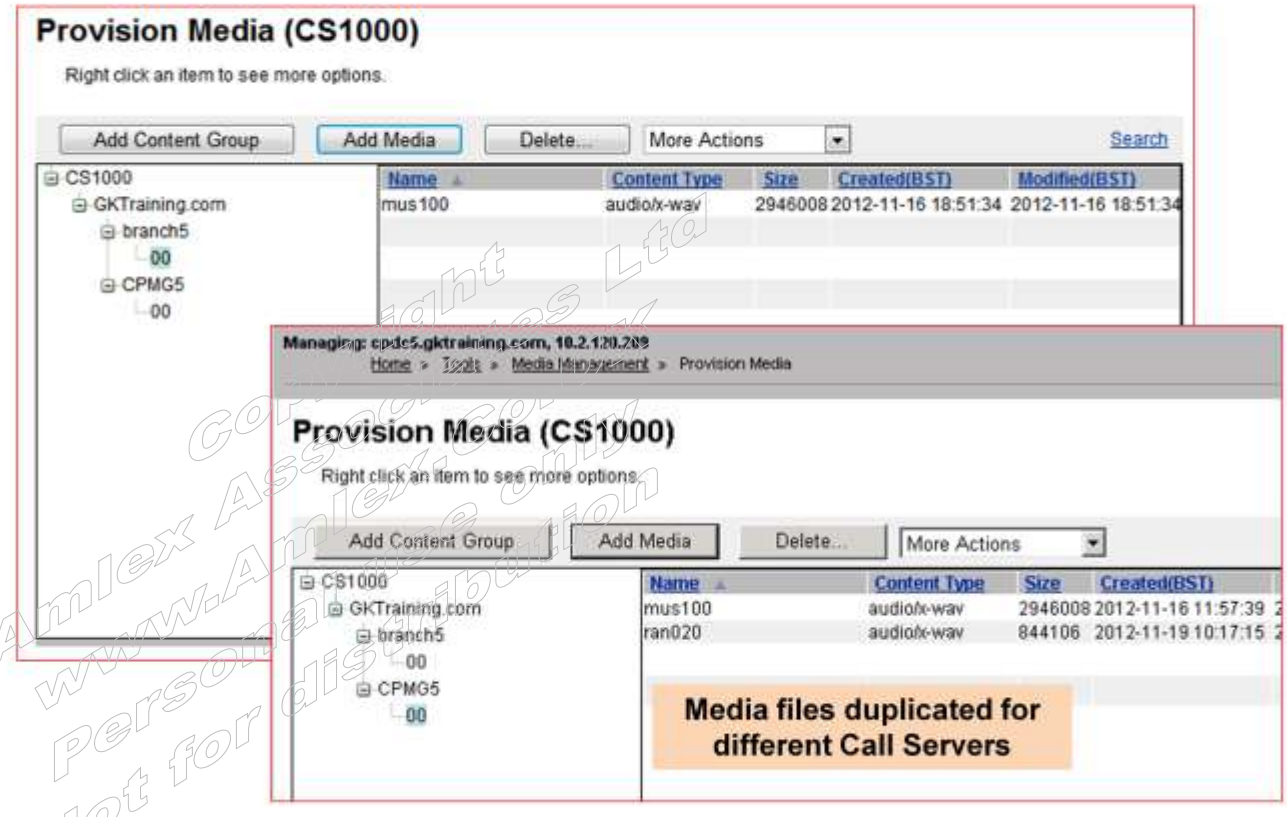
Copyright Amlex Associates Ltd

Media Provision for Multiple Servers

Media is added to the MAS server in exactly the same way as for the Local server except that each individual Call server will have its own folder with its copies of the Media to be played .

As can be seen in these screenshots there are now two separate areas branch5 and cpmg5 and under these each has a customer folder configured (00) to which the media files are uploaded.

NOTE:- because each Call Server has its own copy of media there may be several copies of the same media files on one shared MAS server.



Amlex Associates Ltd Copyright www.Amlex.com Personal use only Not for distribution

Notes

_____

_____

_____

_____

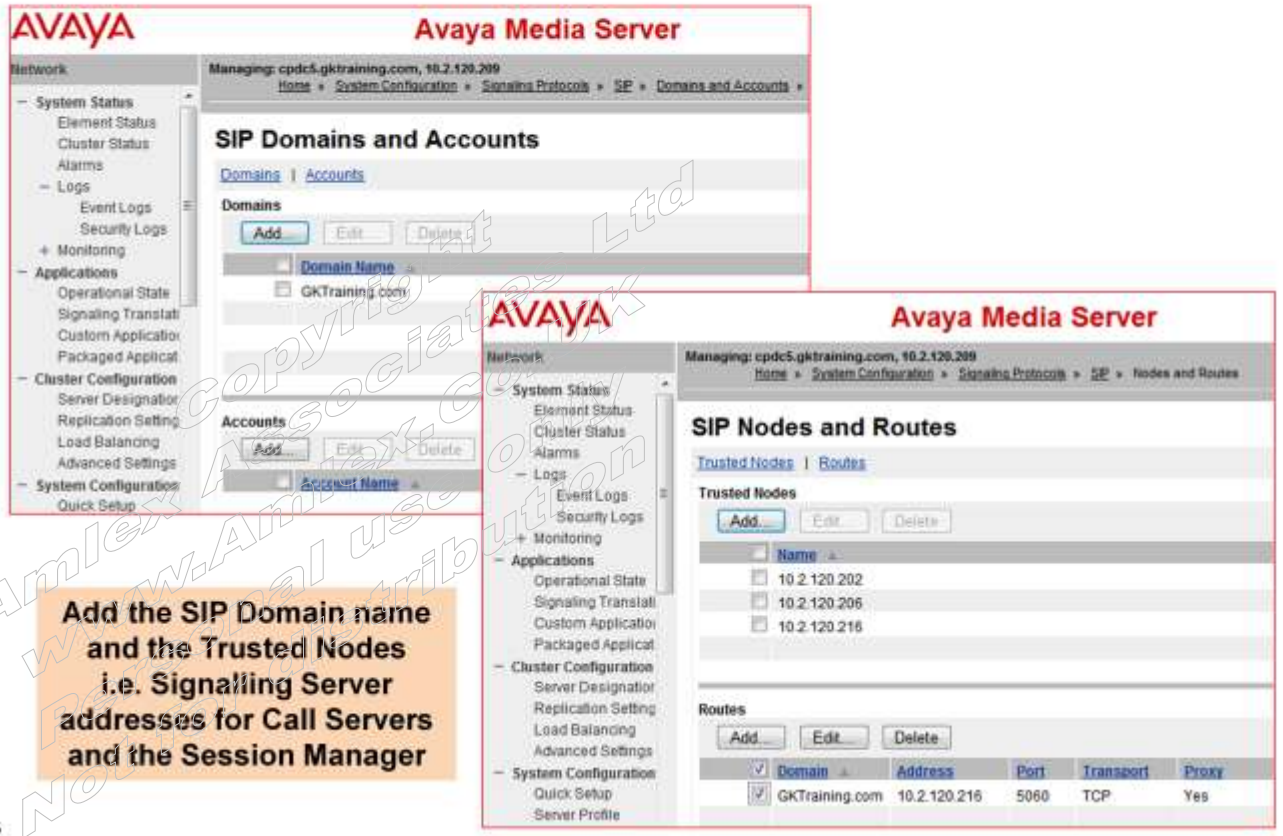
Copyright Amlex Associates Ltd

SIP Domain, Trusted Nodes & Route

The SIP **DOMAIN** name must be defined as it was for the Local Server implementation as it is used to determine file locations.

In addition the MAS will be communicating not only with the Call Servers but also the Session Manager now so we need to ensure that they are all included as **TRUSTED NODES** within the MAS.

Finally we need to add a **SIP ROUTE** to the MAS which defines how we communicate to the Session Manager. See next page.



Amlex Copyright Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

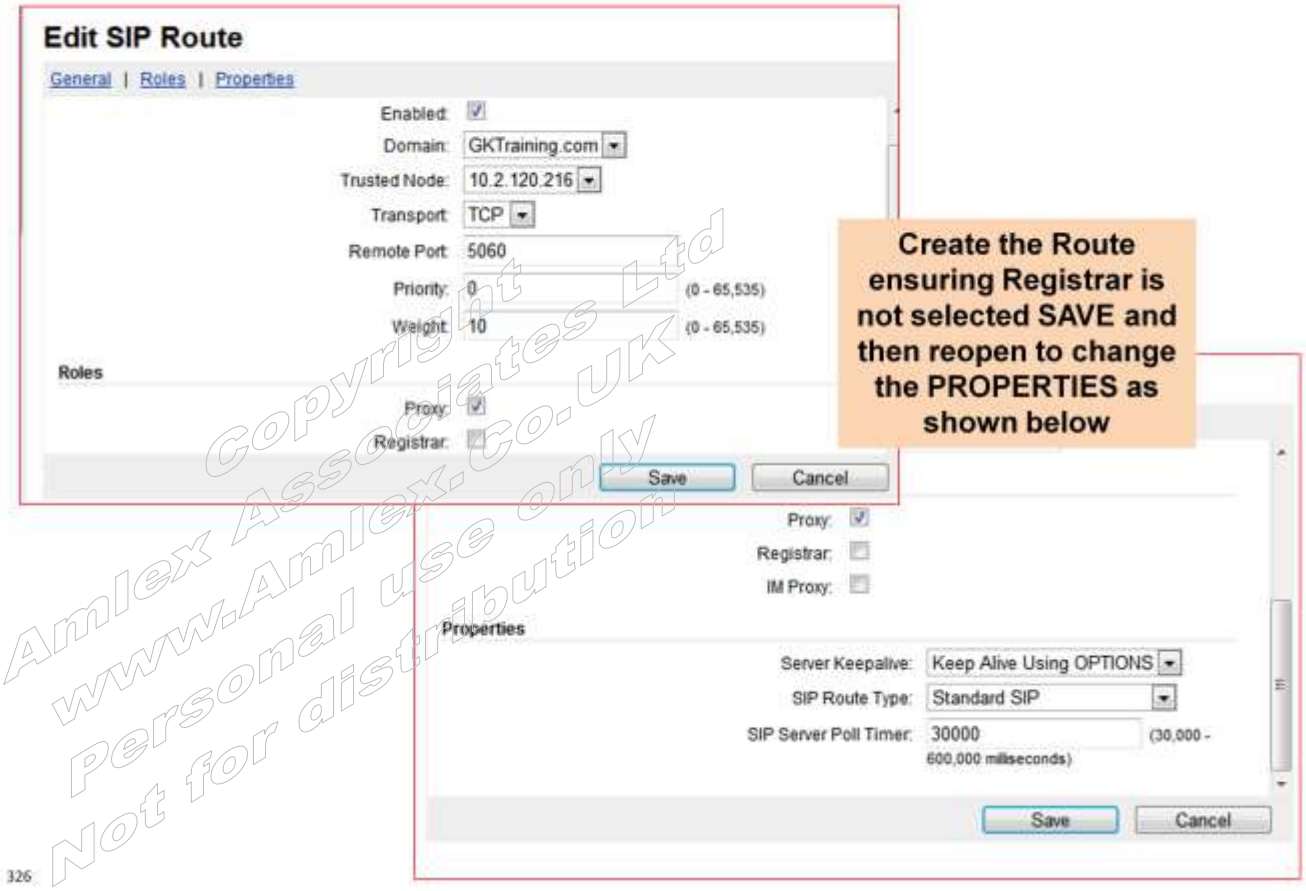
_____

SIP Route

The **SIP ROUTE** defines how we will communicate with the Session Manager so as you can see in these screens we Select the **DOMAIN** from the drop down list as well as the **TRUSTED NOD**E .

The Transport and port numbers will remain at default but the role should only have **PROXY** selected as shown as the Session Manager doesn't use the Registrar function.

You need to save the **ROUTE** at this point and then **EDIT** it again to change the **PROPERTIES** and set the **SERVER KEEPALIVE** to **KEEP ALIVE USING OPTIONS** as shown on the lower screen. **SAVE** the route now to keep these settings.



Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

326

Notes

_____

_____

_____

_____

Locations

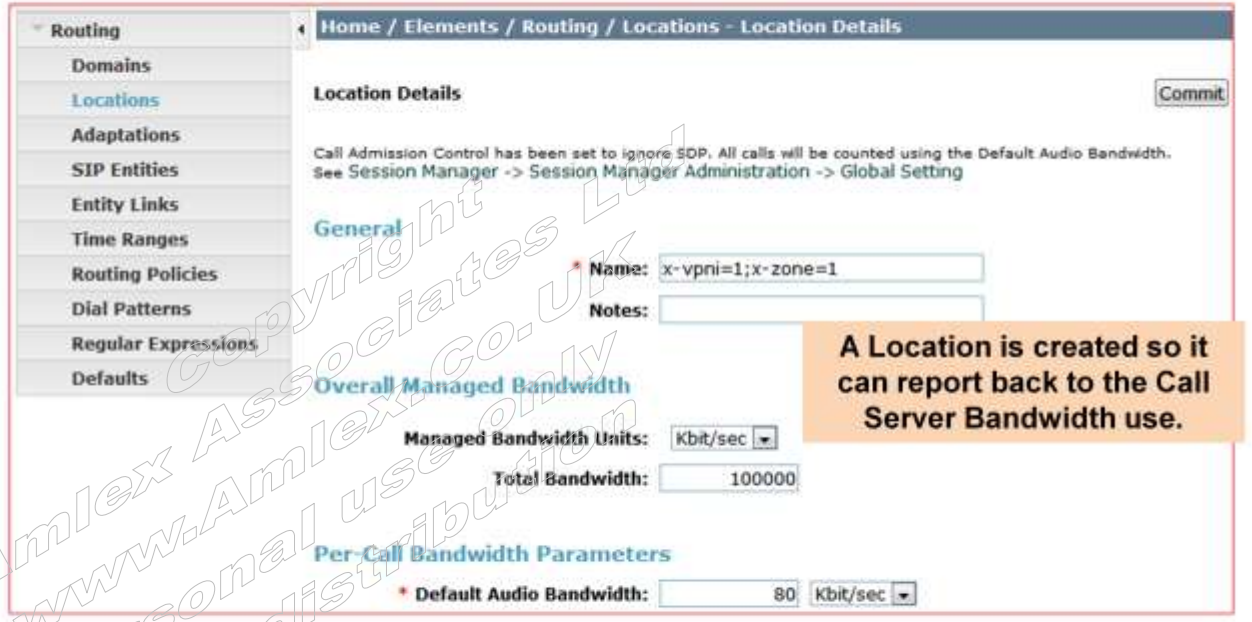
On the Session Manager we now need to configure the SIP Entities and Links etc but first we need to add a **LOCATION** which can be used to control the bandwidth used by the media.

Add the **LOCATION** and use the name as shown :-

x-vpni=1;x-zone=1

These settings can be reported back to the call server for full bandwidth management if required.

Ensure the **TOTAL BANDWIDTH** is set to a realistic figure, in addition you may need to edit the **DEFAULT AUDIO BANDWIDTH** setting as the default is 80Kbps depending on he codecs in use.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

327

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Adaption for MSC

The **ADAPTION** created here will be associated with the two SIP entities for the MSC's on the two Call Servers.

Note that the type is a :-

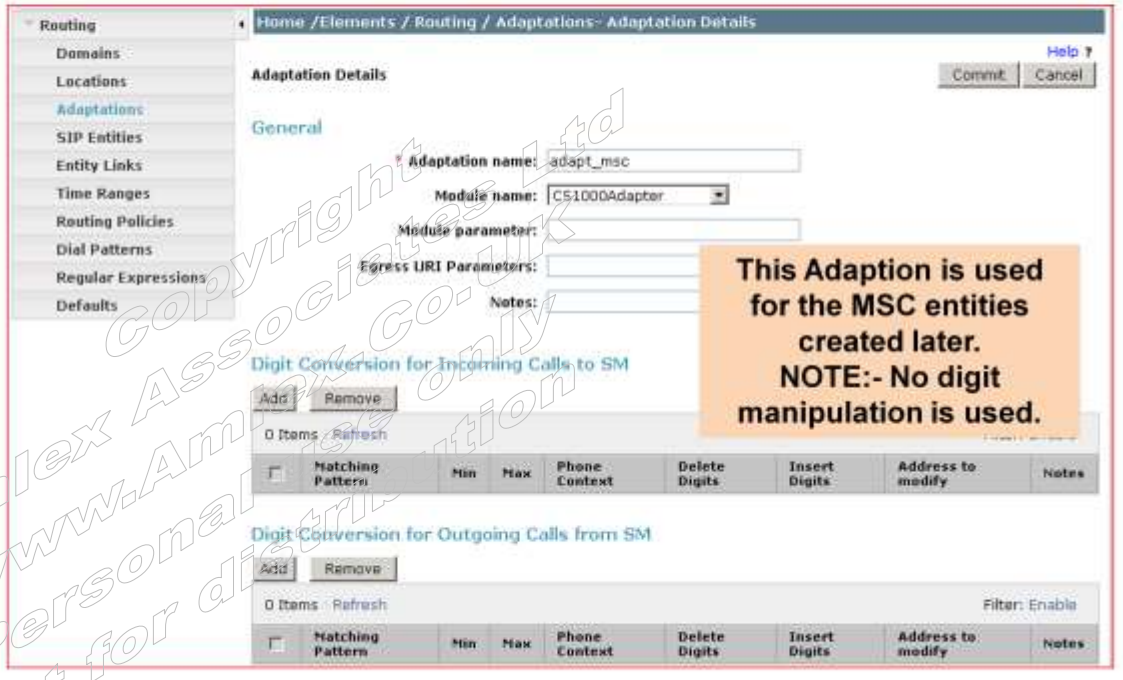
CS1000ADAPTER

But unlike the adaption's built earlier we will not add or delete digits, it will only be used to remove and add back the :-

cdp.udp

Phone context so the Session Manager can route the SIP request correctly.

NOTE:- This adaption can be used for both MSC Entities or separate Adaption's can be created if preferred.



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution
Copyright

328

Notes

_____

_____

_____

_____

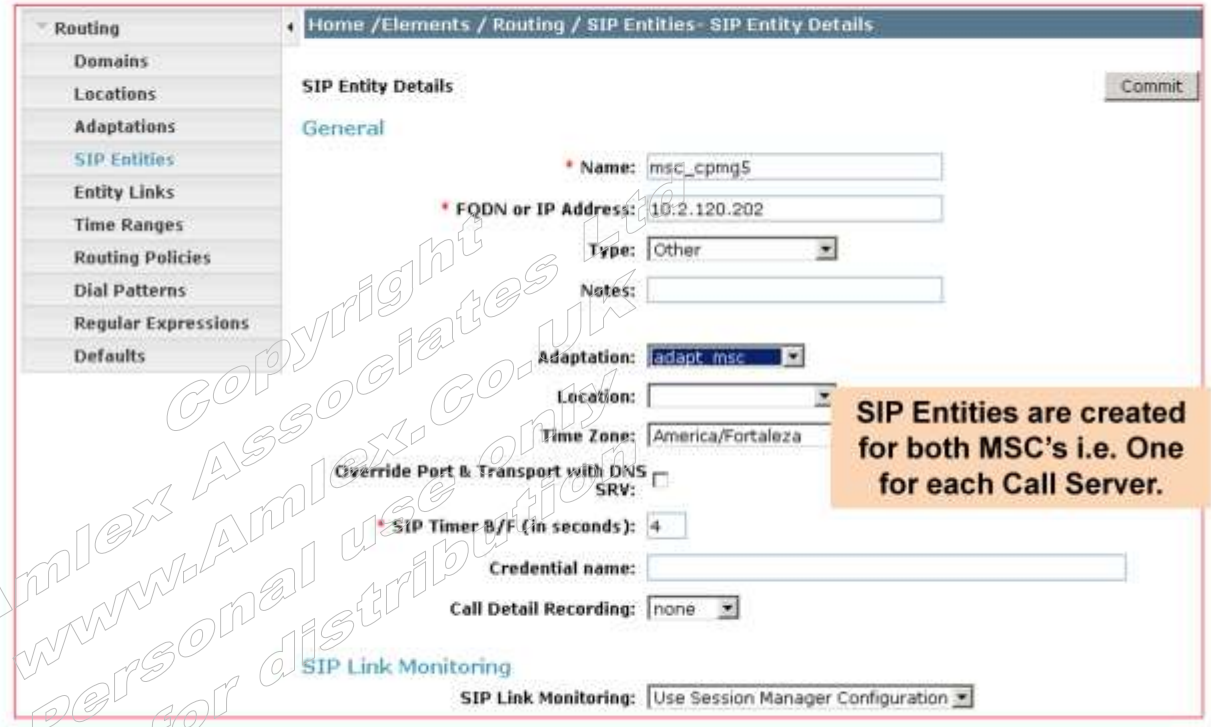
MSC SIP Entity

Even though we have a SIP entity for the Call Server already for call routing, to enable MAS Routing we will also need a SIP Entity for the Media Services Controller on that Call Server.

Here we are adding a new SIP Entity and using the TLAN Signalling Server address to identify it. The **TYPE** will be **OTHER** and we must associate the **ADAPTION** to the MSC Adaption created earlier.

Finally check that the **SIP LINK MONITORING** is set to **USE SESSION MANAGER CONFIGURATION**.

Remember to build SIP entities for all of the MSC's in the network.



Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

329

Notes

_____

_____

_____

_____

Link Entity for MSC

To enable the monitoring of the new Sip Entity we need to create a new **ENTITY LINK.**

The name should reflect the monitored devices and then the **SIP ENTITY 1** and **SIP ENTITY 2** are selected from the drop down menus. Finally set the **PROTOCOL** from its drop down menu to **TCP** which should update the **PORT** number to 5060. If this doesn't happen edit it manually.

The Entity Link is used to monitor the SIP entity and ensure it is available to receive requests.

330

Amlex Copyright www.Amlex-Associates Ltd Personal use only Not for distribution

Notes

_____

_____

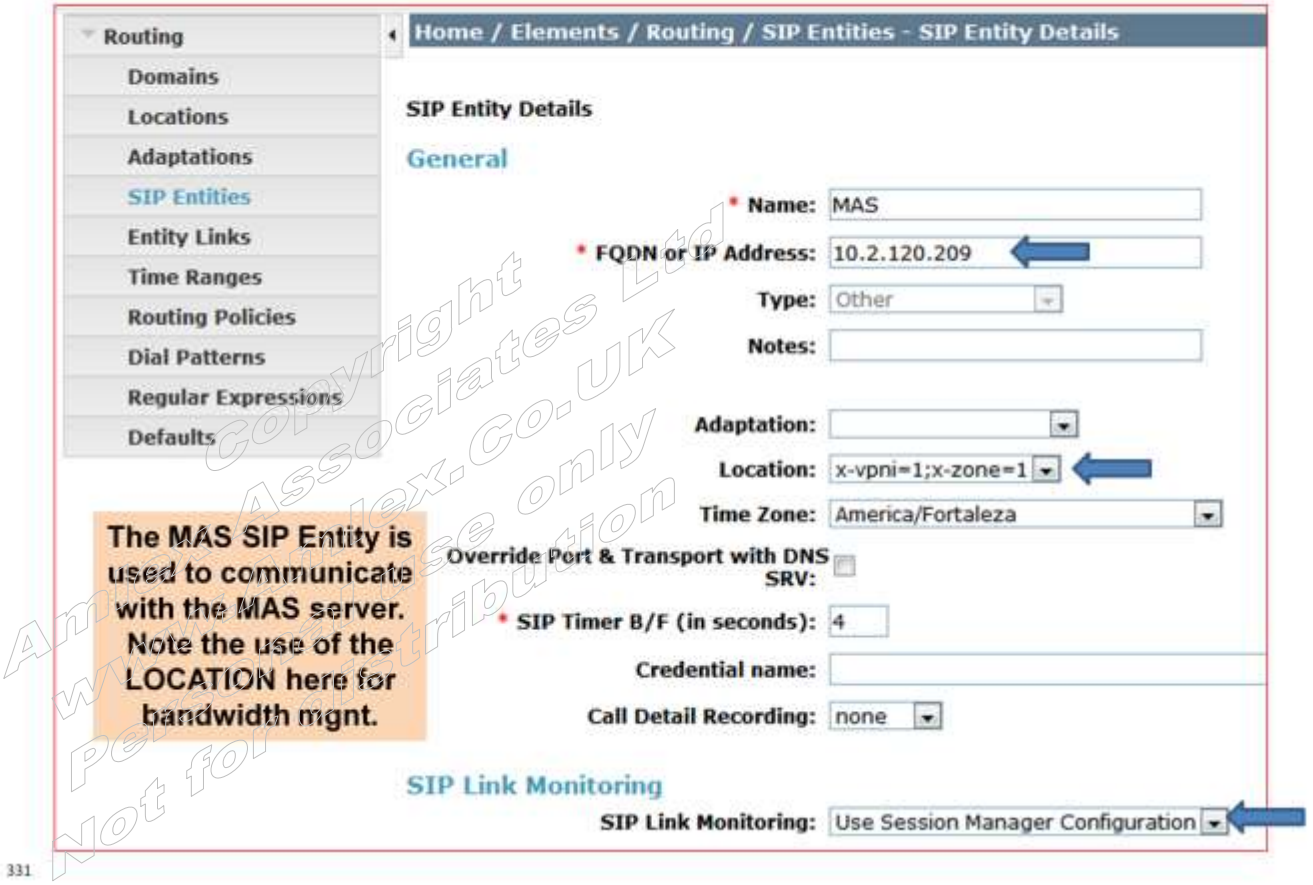
_____

_____

MAS SIP Entity

The MAS SIP Entity is created to allow communication with the MAS server and is not much different from the MSC Entities, except that it uses the **LOCATION** created earlier.

The **FQDN or IP Address** is set to the TLAN IP of the MAS server and no **ADAPTION** is set as we do not need to manipulate the messages received from or sent to the Session Manager



Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

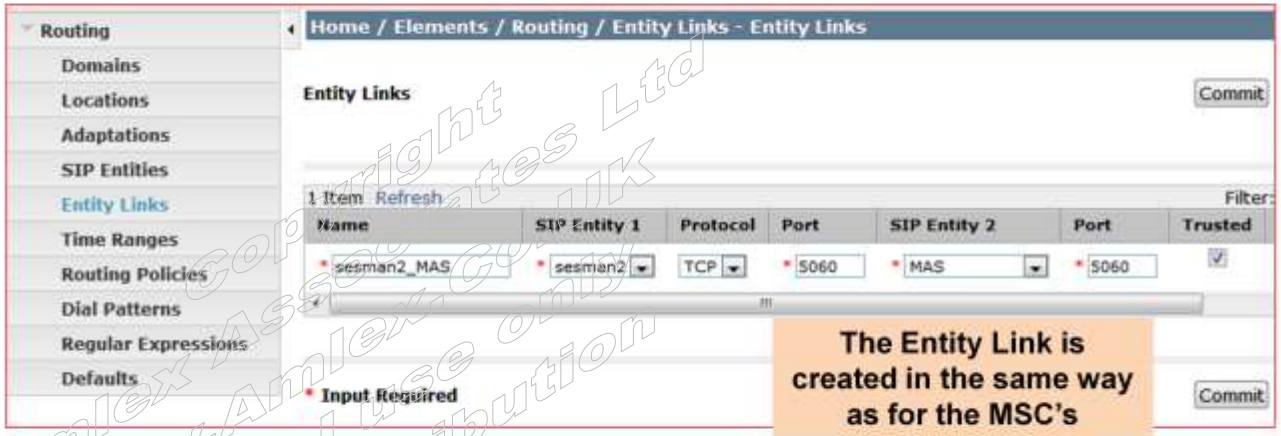
_____

_____

_____

Link Entity for MAS

Again we need to add an ENTITY LINK this time for the MAS server. It is created in the same manner as for the MSC's i.e. From the Session Manager to the MAS using **TCP** on **PORT** 5060



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

332

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Routing Policy

To direct the requests for Media to the MAS we need a **ROUTING POLICY** with an associated Dial Pattern. Routing Policies are found under the Routing tab in the System Manager.

Firstly we add a new policy and select the Destination, in this case the MAS server itself.

The TIME OF DAY is a default 24/7 option but another could be used if required.

Once this is saved using the **COMMIT** button we can move to **DIAL PATTERNS** to add the routing digits.

333

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

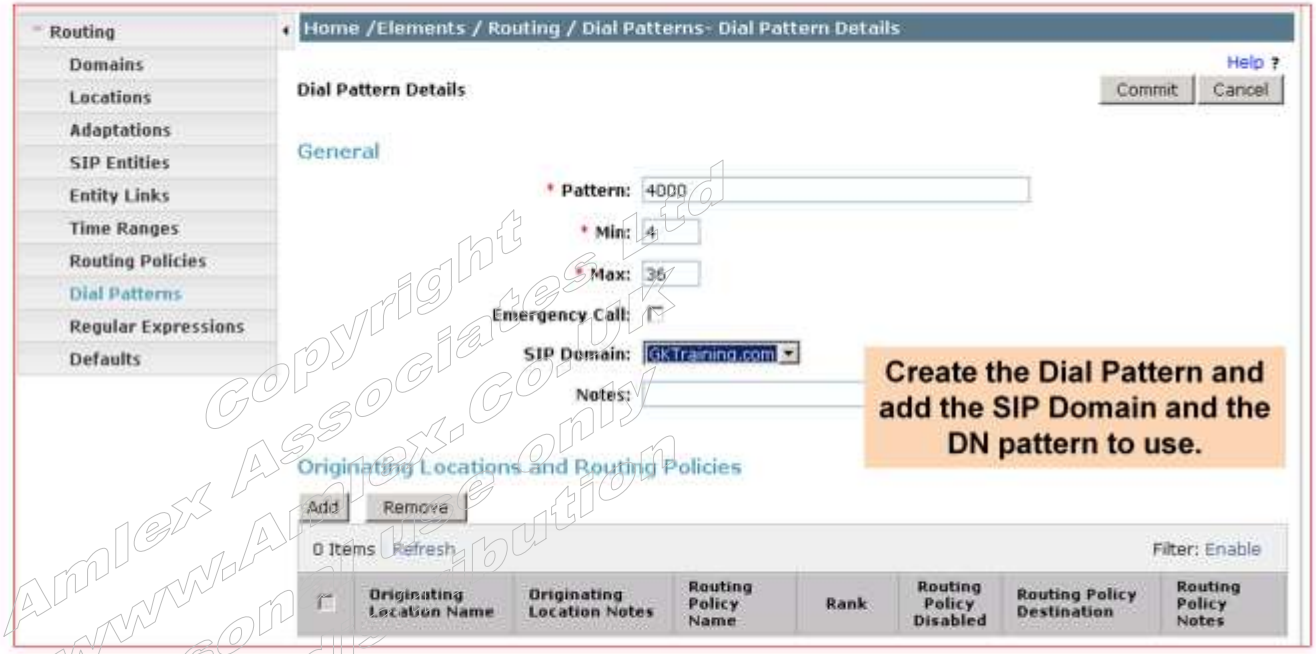
Dial Pattern

First we add a **NEW** Dial Pattern as seen her and enter the **PATTERN** we are routing on.

Here we are using 4000 because that's the number we entered on the Call Server as the MSRN (See following pages).

We will need to increase the **MIN** digits to 4 as we are looking for a 4 digit DN and we also need to select the **SIP DOMAIN.**

Scrolling down the screen we then need to add further details as shown on the next page.



Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

334

Notes

_____

_____

_____

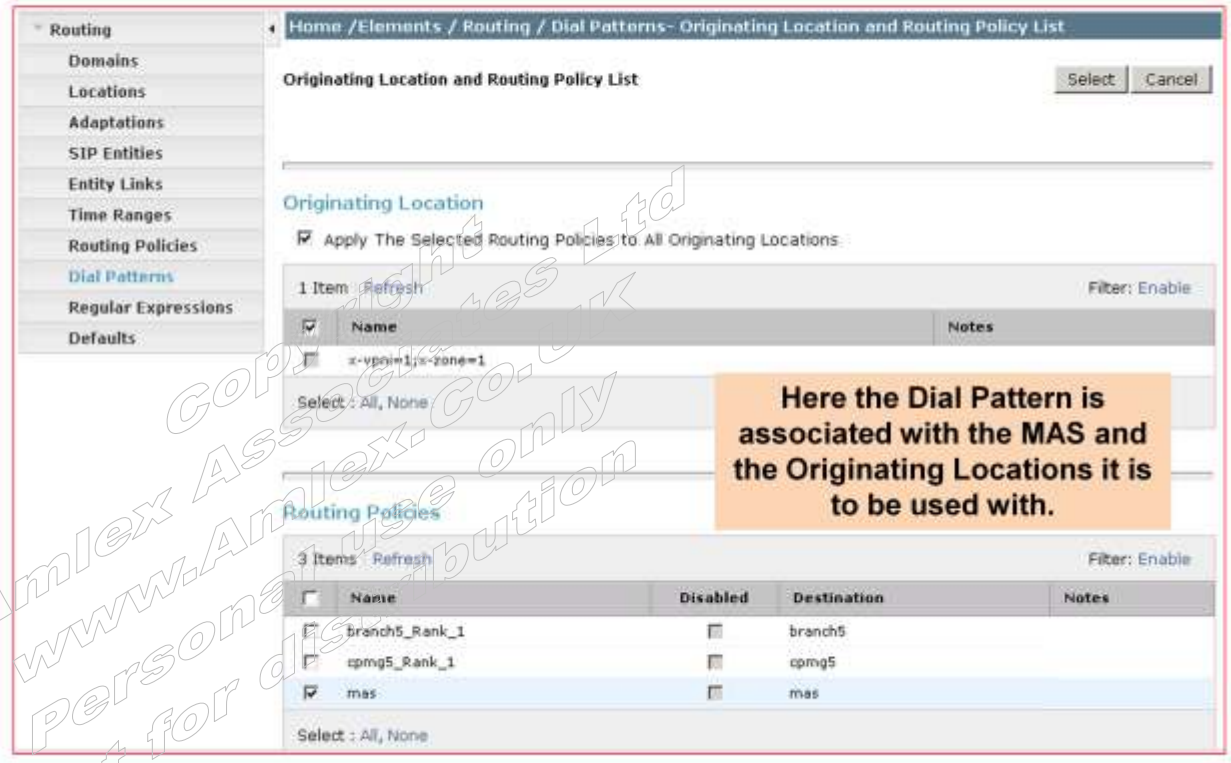
_____

Dial Pattern

The Dial pattern must also have the **ORIGINATING LOCATION** defined and generally you can select the **APPLY THE SELECTED ROUTING POLICIES TO ALL ORIGINATING LOCATIONS** tick box.

Then finally you need to select the **ROUTING POLICIES** the Dial pattern is to be associated with and in the case it will of course be the **MAS** .

This should complete the Session/System Manager configuration for the MAS routing .



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

335

Notes

_____

_____

_____

_____

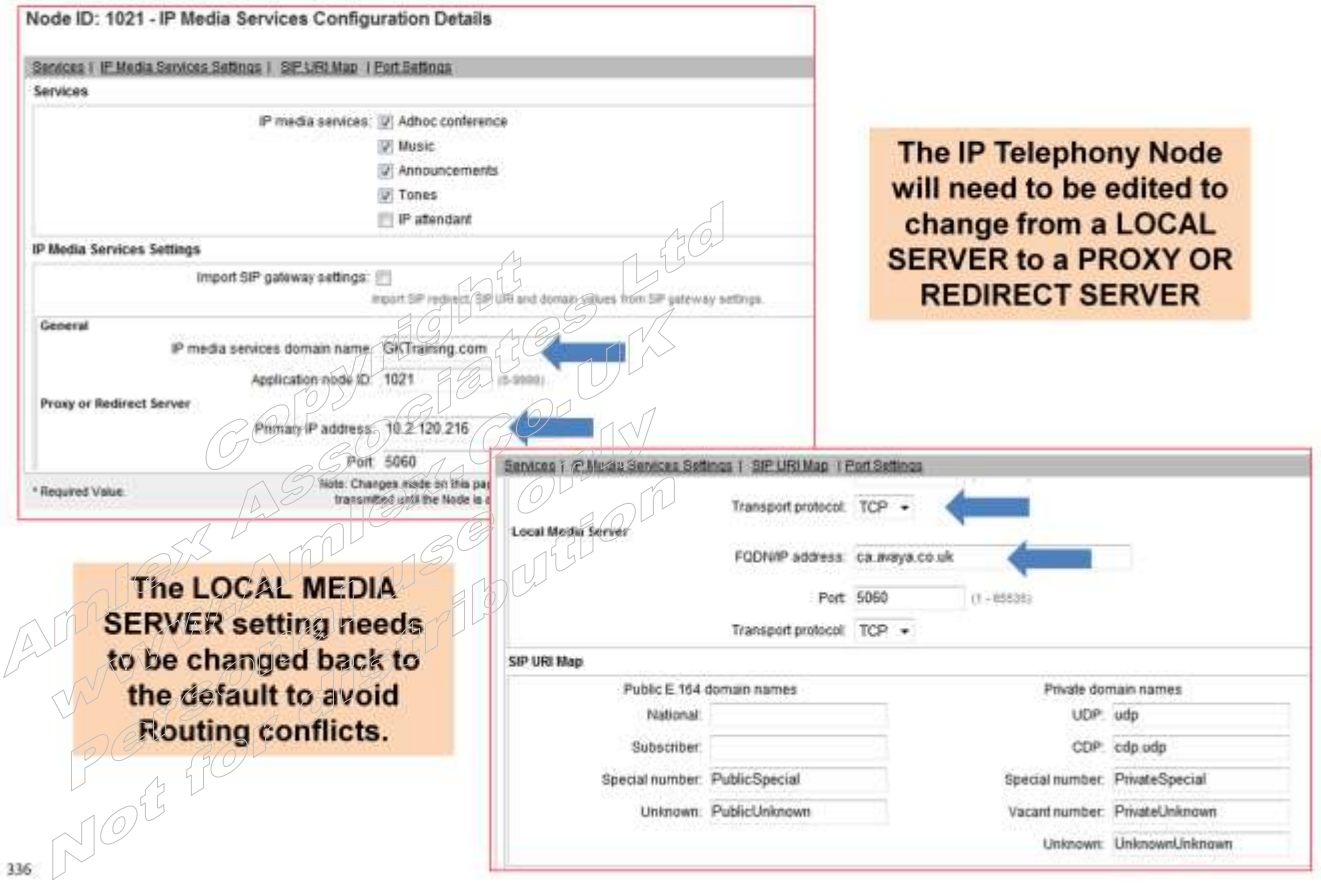
Copyright Amlex Associates Ltd

MSC in IP Node

Back on the Call Server IP Telephony Node we need to edit the Media Services Controller so that it points to the Session Manager now instead of directly to the Local MAS server.

As you can see here the **LOCAL MEDIA SERVER** is reset to the default value as it cannot be left blank and the **PROXY OR REDIRECT SERVER** is set to point at the Session Manager address.

The Domain name should already be configured but if not make sure you add it before you click SAVE and SYNCHRONISE the node. Once Synchronised RESTART the I{P Node to ensure the latest settings are being used.


Node ID: 1021 - IP Media Services Configuration Details
Services | IP Media Services Settings | SIP URI Map | Port Settings
Services
IP media services: Adhoc conference
Music
Announcements
Tones
IP attendant
IP Media Services Settings
Import SIP gateway settings:
General
IP media services domain name: GKTraining.com
Application node ID: 1021
Proxy or Redirect Server
Primary IP address: 10.2.120.216
Port: 5060
* Required Value.
The IP Telephony Node will need to be edited to change from a LOCAL SERVER to a PROXY OR REDIRECT SERVER
Services | IP Media Services Settings | SIP URI Map | Port Settings
Local Media Server
Transport protocol: TCP
FQDN/IP address: ca.avaya.co.uk
Port: 5060
Transport protocol: TCP
SIP URI Map
Public E.164 domain names
National:
Subscriber:
Special number: PublicSpecial
Unknown: PublicUnknown
Private domain names
UDP: udp
CDP: cdp.udp
Special number: PrivateSpecial
Vacant number: PrivateUnknown
Unknown: UnknownUnknown
The LOCAL MEDIA SERVER setting needs to be changed back to the default to avoid Routing conflicts.
336

Copyright Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

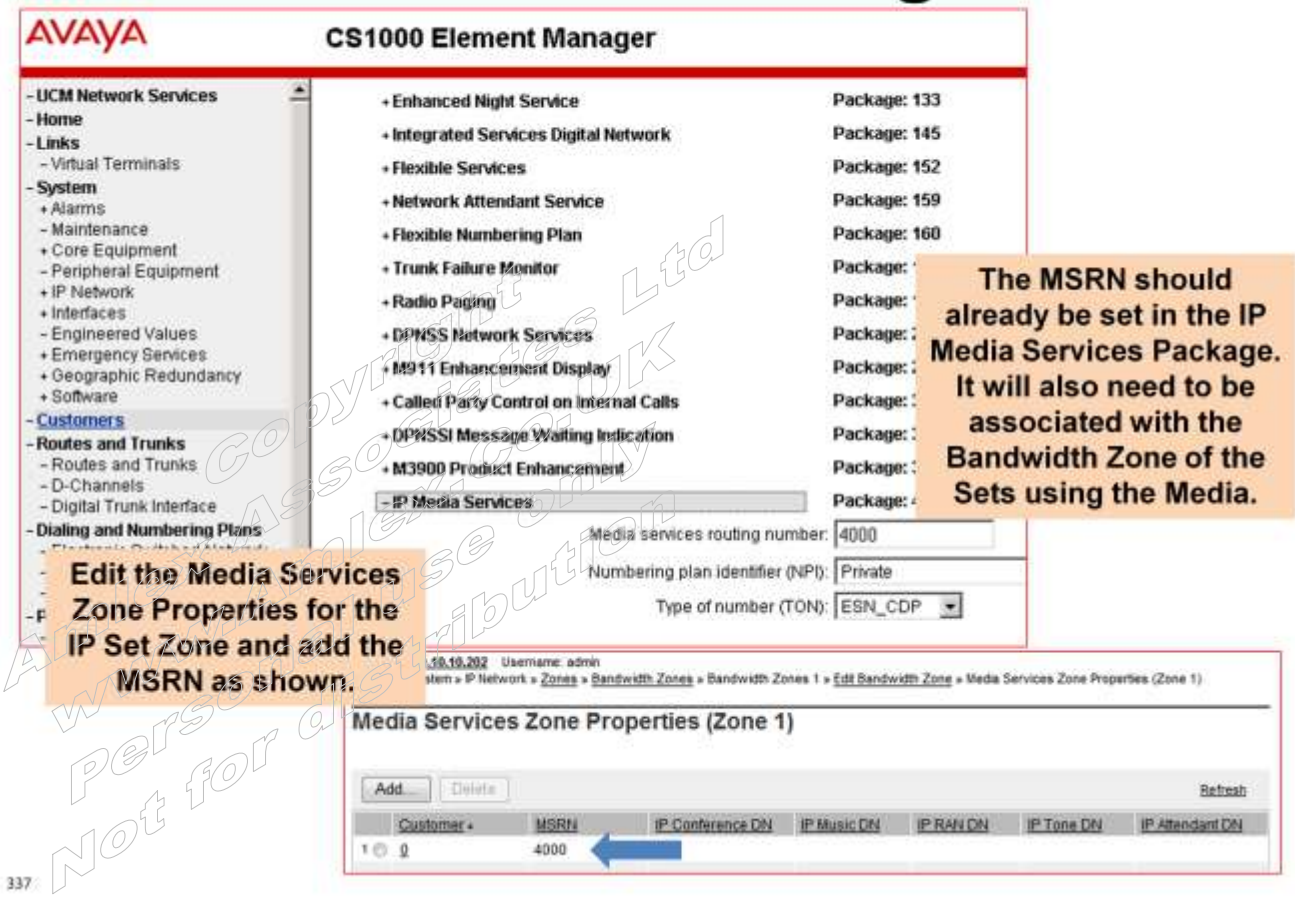
Media Services Routing Number

The Media Services Routing Number (MSRN) was configured earlier into the IP Media Services package as shown here. The DN used is 4000.

What we also need to do is to add the MSRN to the Bandwidth Zone for the IP sets as shown in the lower screenshot.

In the **MEDIA SERVICES ZONE PROPERTIES** you need to at least add the MSRN which is used by the SIP requests and is used to Route them in the Session Manager to the MAS. The other options allow for more DN's to be assigned to different media types which may need to be routed to other servers.

The MAS Routing configuration should now be complete and you can check the SIP requests using the SIP trace tools discussed earlier.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
+ Enhanced Night Service Package: 133
+ Integrated Services Digital Network Package: 145
+ Flexible Services Package: 152
+ Network Attendant Service Package: 159
+ Flexible Numbering Plan Package: 160
+ Trunk Failure Monitor Package:
+ Radio Paging Package:
+ DPNSS Network Services Package:
+ M911 Enhancement Display Package:
+ Called Party Control on Internal Calls Package:
+ DPNSSI Message Waiting Indication Package:
+ M3900 Product Enhancement Package:
- IP Media Services Package:
Media services routing number: 4000
Numbering plan identifier (NPI): Private
Type of number (TON): ESN_CDP
The MSRN should already be set in the IP Media Services Package. It will also need to be associated with the Bandwidth Zone of the Sets using the Media.
Edit the Media Services Zone Properties for the IP Set Zone and add the MSRN as shown.
Media Services Zone Properties (Zone 1)
Add... Delete Refresh
Customer MSRN IP Conference DN IP Music DN IP RAN DN IP Tone DN IP Attendant DN
1 0 4000

Amlex Associates Ltd Copyright Personal use only Not for distribution

Notes

_____

_____

_____

_____

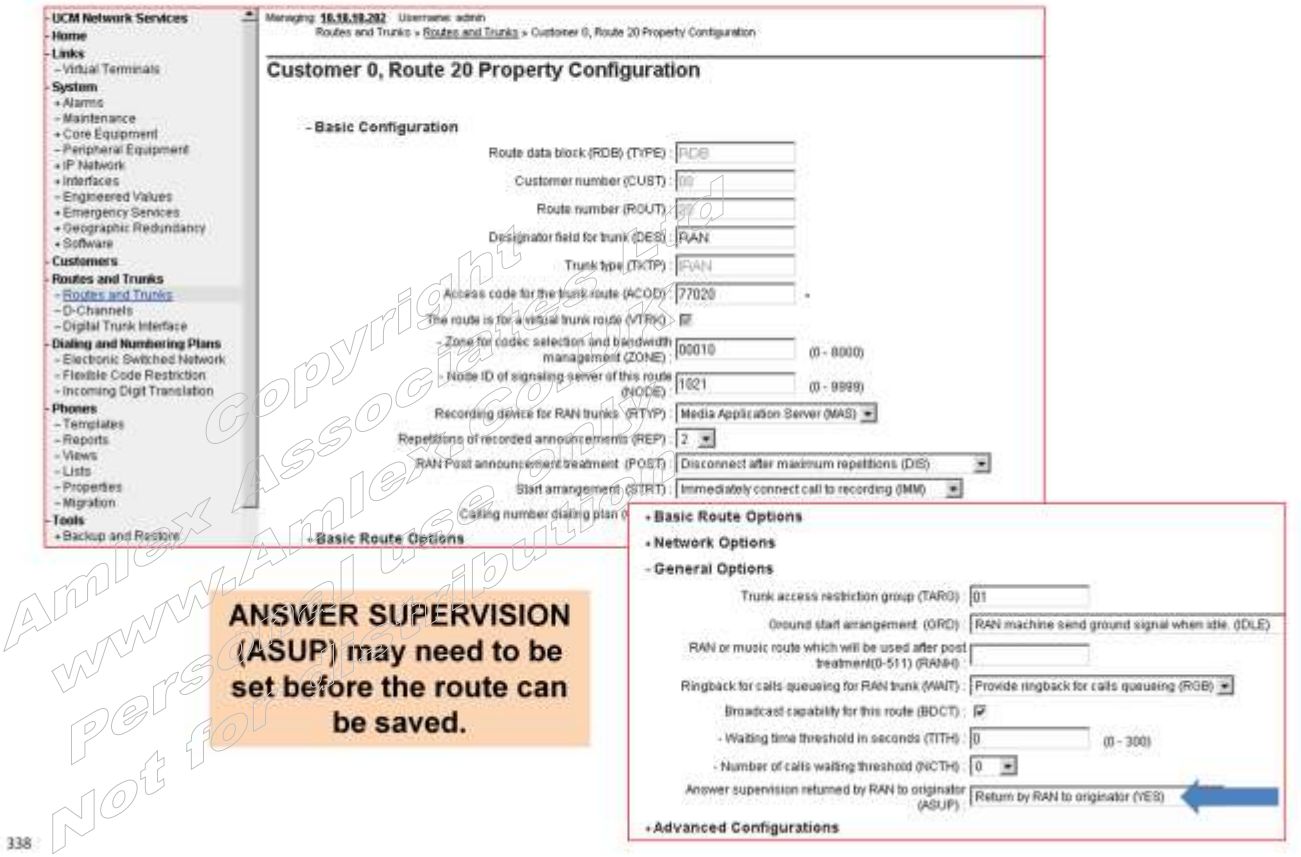
RAN Configuration

In addition to Music on Hold Announcements may also be served from the MAS.

The screenshots show configuration of an IRAN Route which is very similar to the Music on Hold example. Note that you may need to select Answer Supervision (ASUP) to complete the configuration of the route.

The route will need to have Trunks assigned to it before it can be used, again these are much the same as the IMUS trunks.

To test the operation of the announcement you can access it directly using the Route ACOD.


UCM Network Services
Home
Links
Virtual Terminals
System
Alarms
Maintenance
Core Equipment
Peripheral Equipment
IP Network
Interfaces
Engineered Values
Emergency Services
Geographic Redundancy
Software
Customers
Routes and Trunks
Routes and Trunks
D-Channels
Digital Trunk Interface
Dialing and Numbering Plans
Electronic Switched Network
Flexible Code Restriction
Incoming Digit Translation
Phones
Templates
Reports
Views
Lists
Properties
Migration
Tools
Backup and Restore
Routes and Trunks » Routes and Trunks » Customer 0, Route 20 Property Configuration
Customer 0, Route 20 Property Configuration
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 00
Route number (ROUT) : 20
Designator field for trunk (DES) : RAN
Trunk type (TKTP) : IRAN
Access code for the trunk route (ACOD) : 77020
The route is for a virtual trunk route (VTRK) :
Zone for codec selection and bandwidth management (ZONE) : 00010 (0 - 8000)
Node ID of signaling server of this route (NODE) : 1021 (0 - 9999)
Recording device for RAN trunks (RTYP) : Media Application Server (MAS)
Repetitions of recorded announcements (REP) : 2
RAN Post announcement treatment (POST) : Disconnect after maximum repetitions (DIS)
Start arrangement (STRT) : Immediately connect call to recording (IMM)
+ Basic Route Options
+ Network Options
- General Options
Trunk access restriction group (TARG) : 01
Ground start arrangement (GRD) : RAN machine send ground signal when idle. (IDLE)
RAN or music route which will be used after post treatment(0-511) (RANH) :
Ringback for calls queueing for RAN trunk (WAIT) : Provide ringback for calls queueing (RGB)
Broadcast capability for this route (BDCT) :
- Waiting time threshold in seconds (TITH) : 0 (0 - 300)
- Number of calls waiting threshold (NCTH) : 0
Answer supervision returned by RAN to originator (ASUP) : Return by RAN to originator (YES)
+ Advanced Configurations
ANSWER SUPERVISION (ASUP) may need to be set before the route can be saved.
338

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

27. Maintenance & Diagnostics

- Log Files
  - Call Server
  - UCM
- Hunt Groups
- Backup UCM
  - Follower SS
- Call Server Backups
  - USB Memory Stick
  - FTP Server
- Personal Directory
  - Backup
- IP Set Diagnostics
- IP Phone Firmware
- Tracking Calls
- Monitoring D Channel

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

339

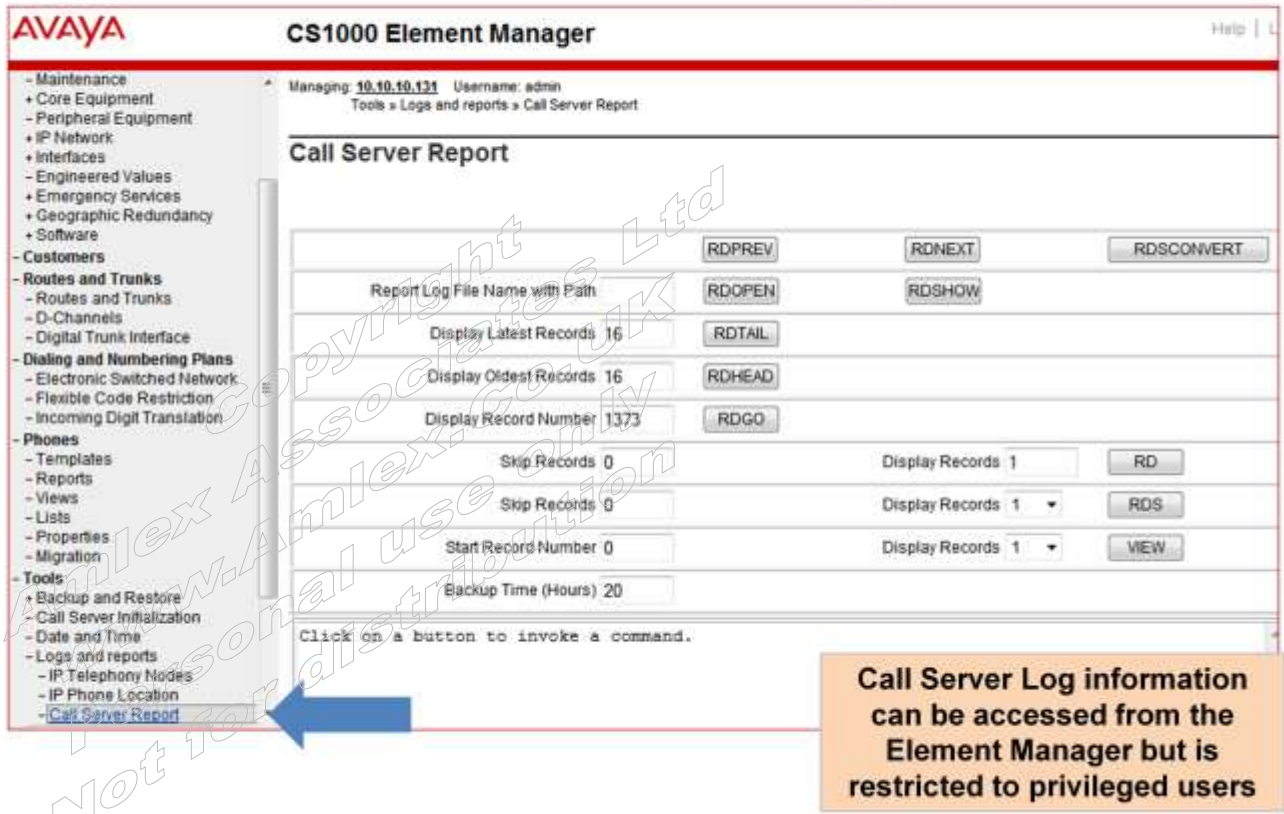
Notes

Call Server Logs

The Call server logs can be accessed from the Element Manager or the PDT mode (Problem Determination Tool) . As PDT is restricted the Element manager offers the best option.

The Reports are accessed from the **TOOLS / CALL SERVER REPORT** menu item.

Once you are at the screen shown you can use the buttons on the display to look at the HEAD and TAIL of the file or specific records.



Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

340

Notes

_____

_____

_____

_____

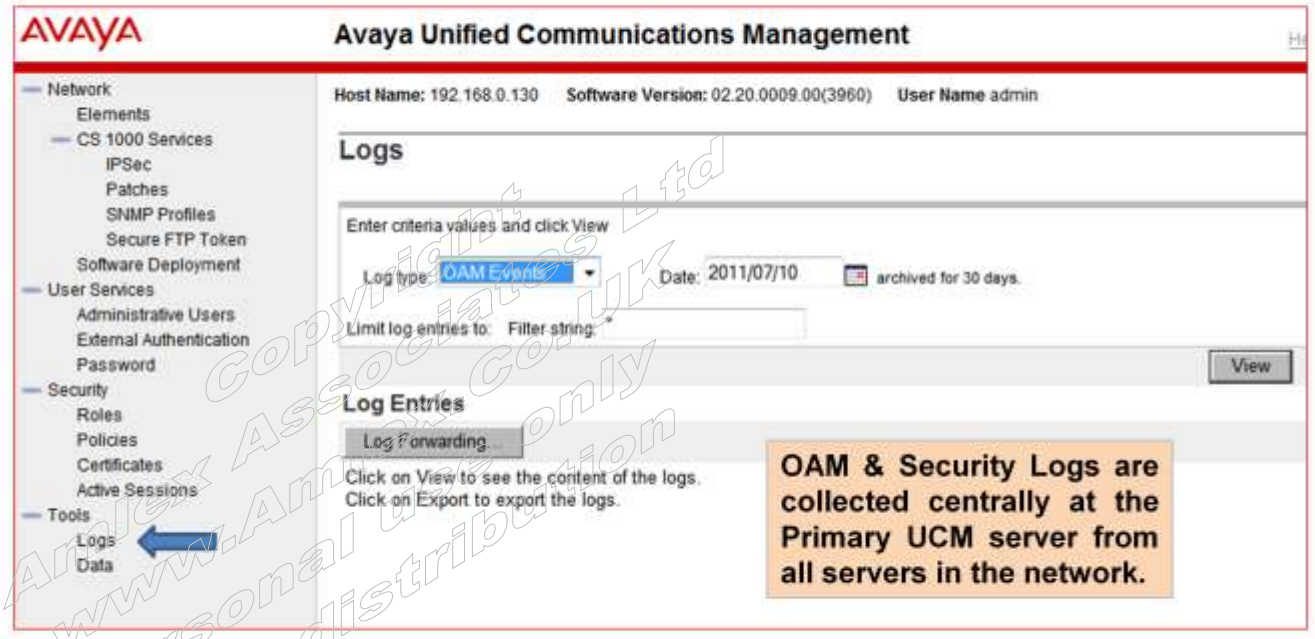
OAM & Security Logs – Primary UCM

The Primary UCM server collects both OAM and Security logs from all the Linux servers in the security domain.

These can be accessed from the UCM as shown here **TOOLS / LOGS** and are collected over a period of time.

In addition the logs can be forwarded to a third party Syslog server or alternatively Exported to a CSV format file.

Centralised collection allows the administrator to view the total domain through one portal.



341

Notes

_____

_____

_____

_____

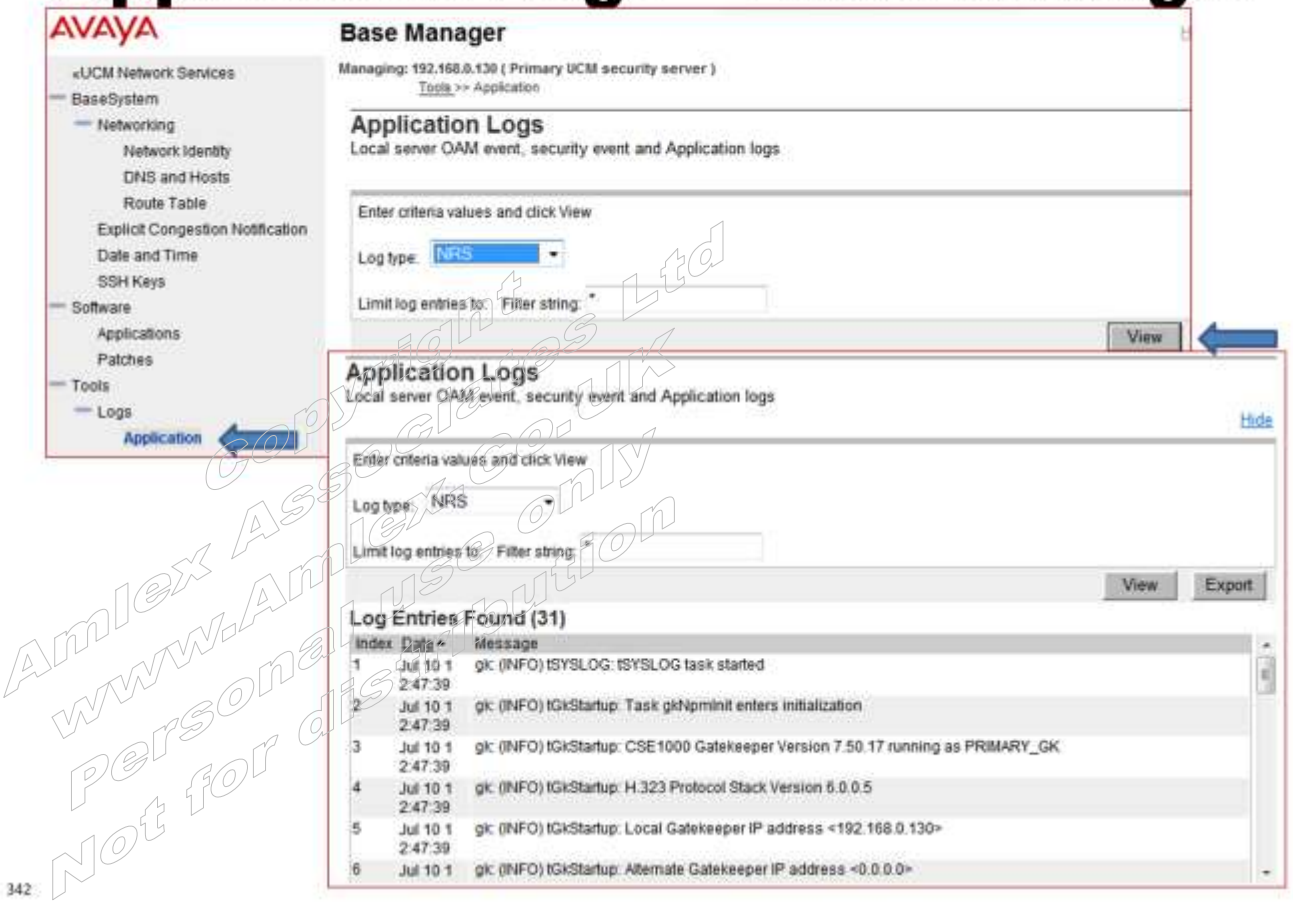
Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Application Logs – Base Manager

The Application logs for the Linux servers are collected on each individual server.

They are accessed by navigating to the Linux Base as shown here and then selecting the **TOOLS / LOGS / APPLICATION** option on the menu.

The LOG TYPE drop down Menu shows the different Log files available and again they may be viewed or exported.



Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

On the CoRes call Server if a USB stick is inserted in the CPPM card the system will automatically send the EDD backup to it rather than the Compact Flash card.

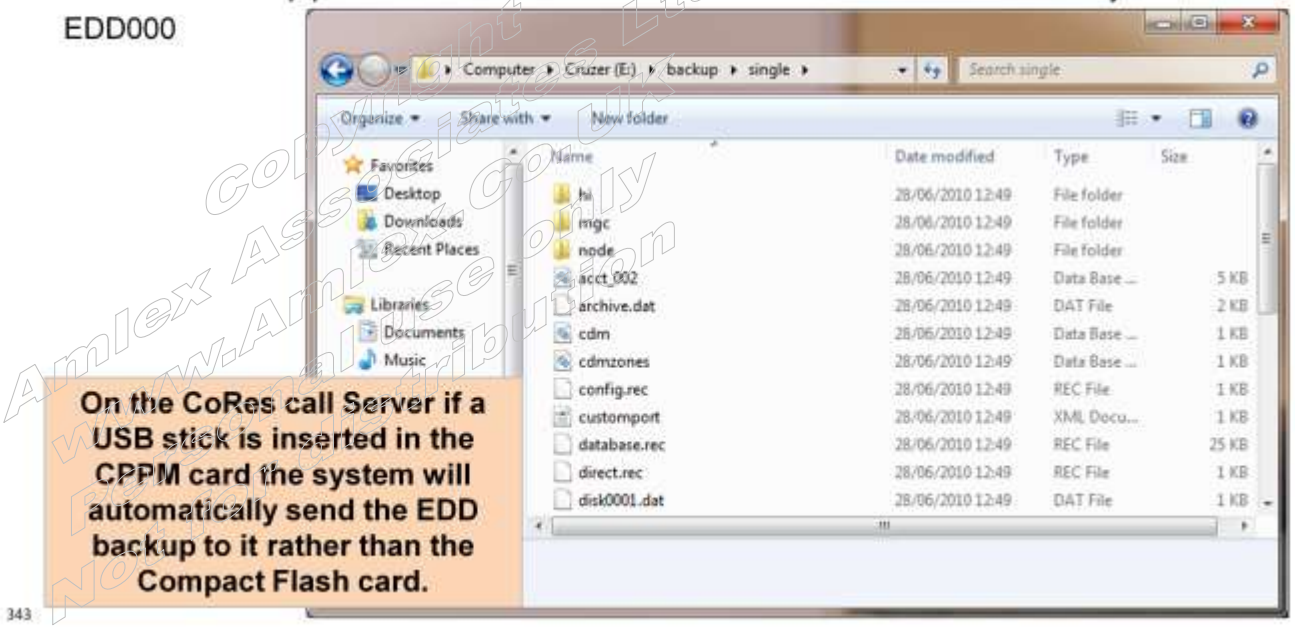
You can see the dialogue (Top) which shows this . The screenshot shows the backup on the USB memory stick itself.

This makes an easy option to capture a Call Server backup for retention or transfer.

Note :-
The USB does not need to be mounted in Linux for the backup to be saved to it.

CoRes CS USB Backup

Backing up reten.bkp
Starting database backup
to local Removable Media Device
Backing up reten.bkp to "/var/opt/nortel/cs/fs/usb/backup/single"
Database backup Complete!
TEMU207 Backup process to local Removable Media Device ended successfully.
EDD000


Computer ▸ Cruzer (E:) ▸ backup ▸ single ▸
Search single
Organize
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Name
Date modified
Type
Size
hi 28/06/2010 12:49 File folder
mgc 28/06/2010 12:49 File folder
node 28/06/2010 12:49 File folder
acct_002 28/06/2010 12:49 Data Base ... 5 KB
archive.dat 28/06/2010 12:49 DAT File 2 KB
cdm 28/06/2010 12:49 Data Base ... 1 KB
cdmzones 28/06/2010 12:49 Data Base ... 1 KB
config.rec 28/06/2010 12:49 REC File 1 KB
customport 28/06/2010 12:49 XML Docu... 1 KB
database.rec 28/06/2010 12:49 REC File 25 KB
direct.rec 28/06/2010 12:49 REC File 1 KB
disk0001.dat 28/06/2010 12:49 DAT File 1 KB
On the CoRes call Server if a USB stick is inserted in the CPPM card the system will automatically send the EDD backup to it rather than the Compact Flash card.
343

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Call Server FTP backup

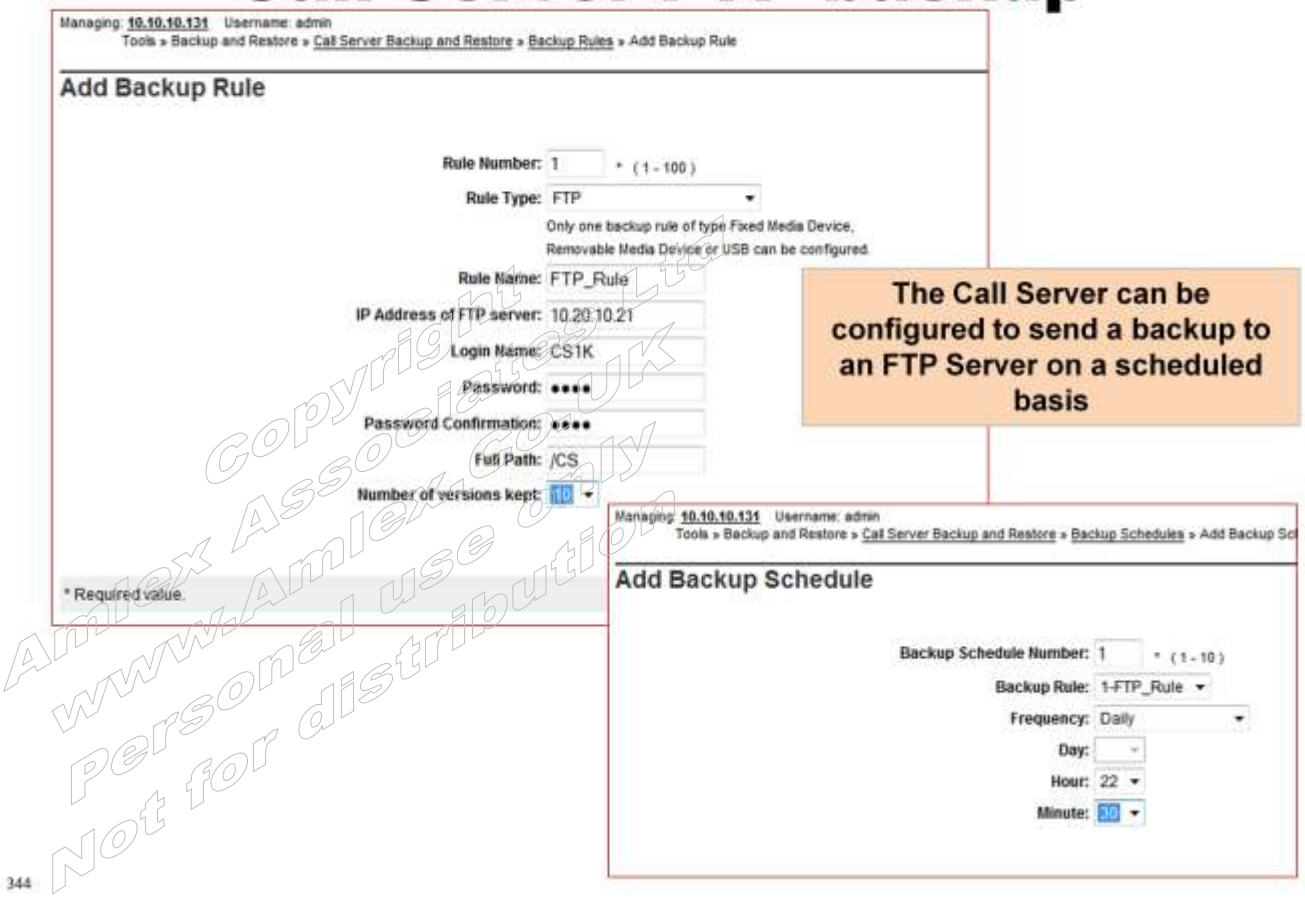
The Call Server can be configured to send a backup file to an FTP server using a backup rule. To have this occur on a regular basis the rule can be executed by a backup schedule.

The Backup Rule and Schedules screens are accessed from Element Manager using the option TOOLS / BACKUP AND RESTORE / CALL SERVER BACKUP AND RESTORE. The FTP rule can also be created in LD 117.

When creating the rule you need to specify the server address, login details, the full path (Directory) on the server and the number of backup to keep.

The schedule allows for different frequencies of execution of the backup rule.

Note:-
This is only a Call Server Backup not a full UCM backup and can be configured for Cores, SA and HA systems.


Managing: 10.10.10.131 Username: admin
Tools » Backup and Restore » Call Server Backup and Restore » Backup Rules » Add Backup Rule
Add Backup Rule
Rule Number: 1 * (1 - 100)
Rule Type: FTP
Only one backup rule of type Fixed Media Device, Removable Media Device or USB can be configured.
Rule Name: FTP_Rule
IP Address of FTP server: 10.20.10.21
Login Name: CS1K
Password: ••••
Password Confirmation: ••••
Full Path: /CS
Number of versions kept: 10
* Required value.
The Call Server can be configured to send a backup to an FTP Server on a scheduled basis
Managing: 10.10.10.131 Username: admin
Tools » Backup and Restore » Call Server Backup and Restore » Backup Schedules » Add Backup Sc
Add Backup Schedule
Backup Schedule Number: 1 * (1 - 10)
Backup Rule: 1-FTP_Rule
Frequency: Daily
Day:
Hour: 22
Minute: 30
344

Copyright Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

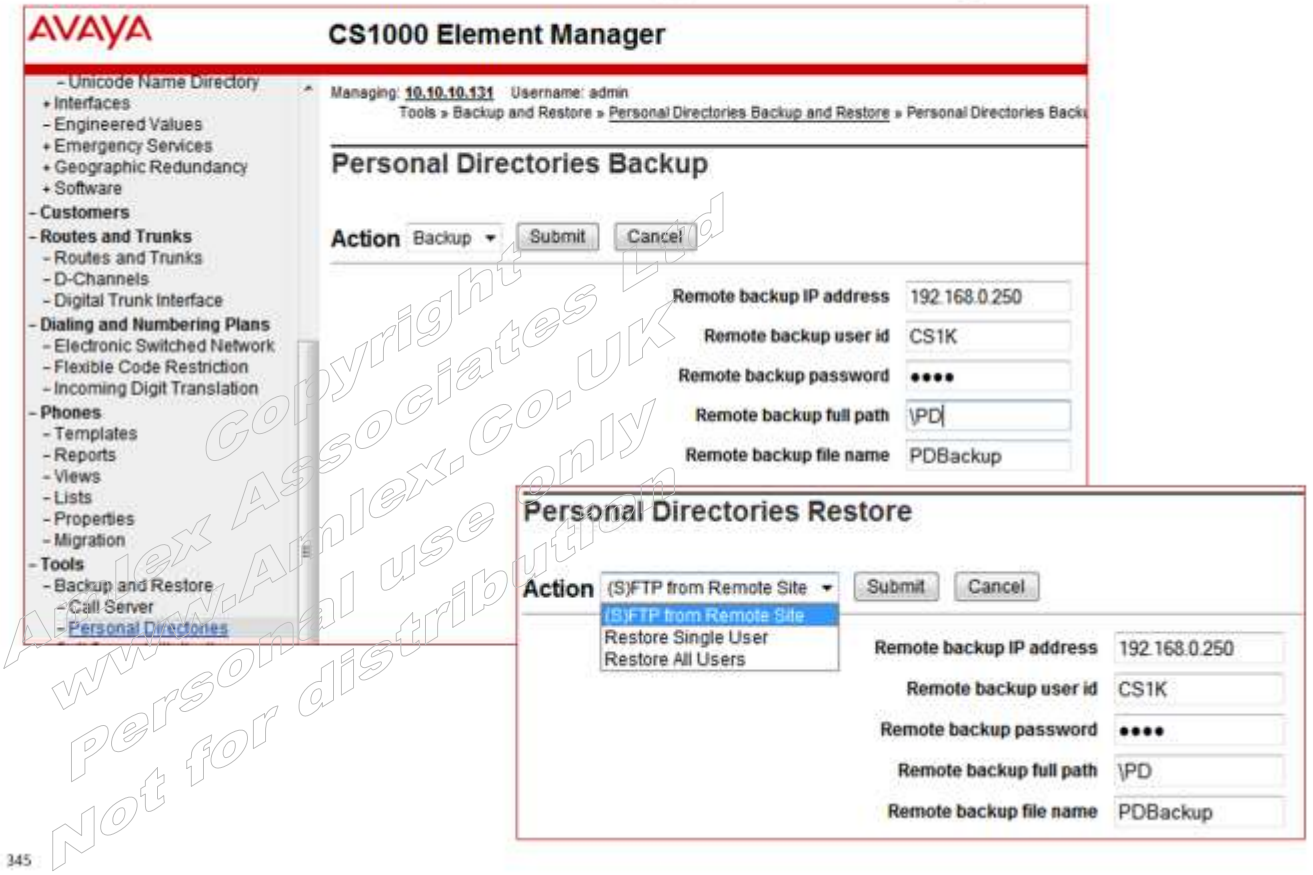
Personal Directory Backup/Restore

To backup or restore the Personal Directory you need to have available a Secure FTP (SFTP) server on the network e.g. Cerberus.

To access the Personal Directory backup got to TOOLS / BACKUP AND RESTORE / PERSONAL DIRECTORIES BACKUP AND RESTORE.

The backup destination is added along with the User ID and password and the backup directory and filename.

To restore a Personal Directory is a two stage process (Lower screenshot). Firstly you move the file back from the remote server using FTP (Shown) . This makes it available but you must then choose to restore either individual users or all users.



Amlex Associates Ltd Copyright www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

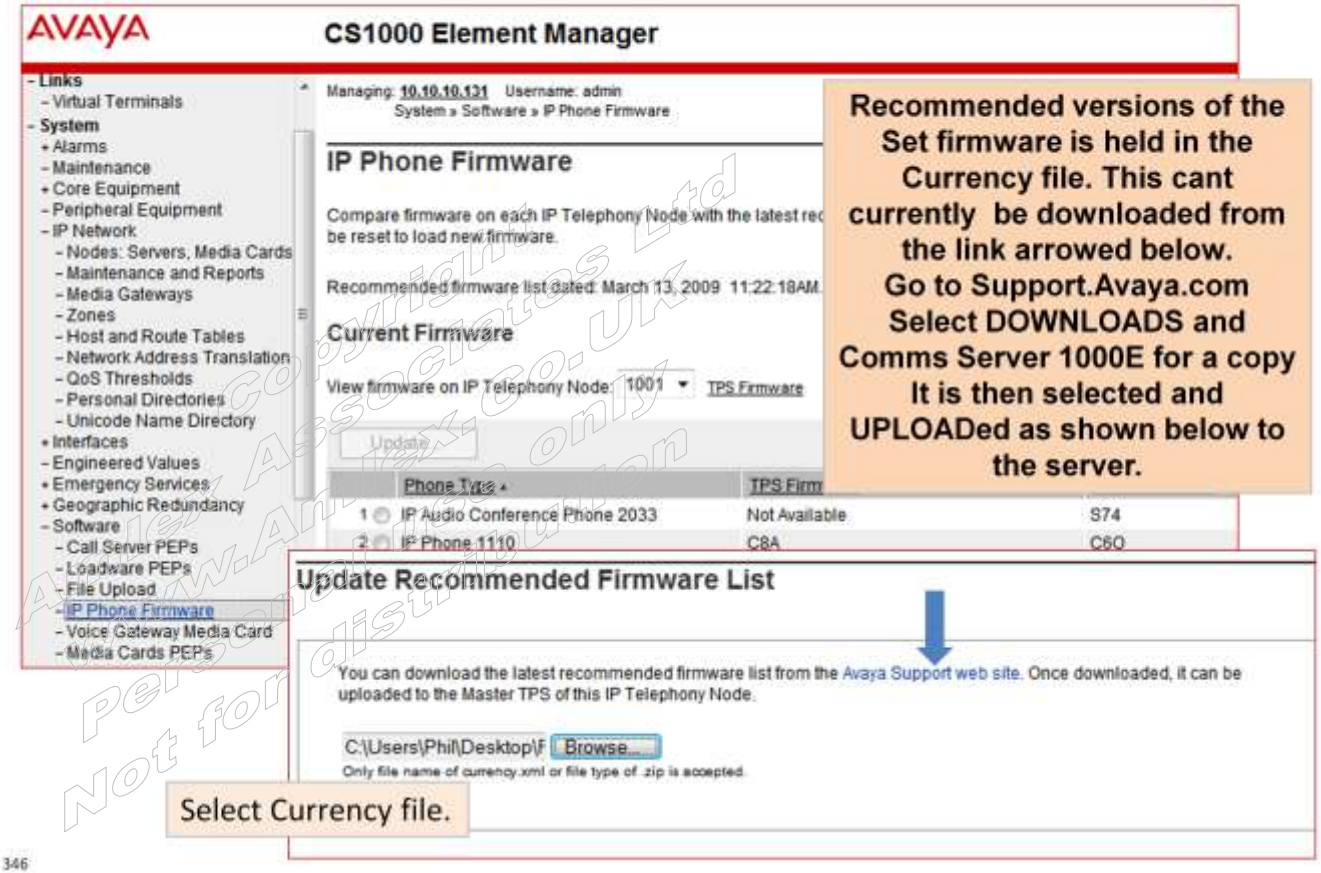
_____

Phone Firmware is an important part of the system and needs to be kept current.

This can be done using a terminal linked to both the EM and the Internet. By clicking on the Links (In Blue) the system will automatically try to download the requested file. Currently the Firmware Currency file is not available on the Avaya site. Go to Support.Avaya.Com and select DOWNLOADS for Communications Server 1000E to access the file.

The Currency file is a list of the latest firmware available and this should be updated first. From this you can select which devices need new firmware.

IP Phone Firmware


AVAYA
CS1000 Element Manager
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
- Software
- Call Server PEPs
- Loadware PEPs
- File Upload
- IP Phone Firmware
- Voice Gateway Media Card
- Media Cards PEPs
Managing: 10.10.10.131 Username: admin
System » Software » IP Phone Firmware
IP Phone Firmware
Compare firmware on each IP Telephony Node with the latest rec
be reset to load new firmware.
Recommended firmware list dated: March 13, 2009 11:22:18AM
Current Firmware
View firmware on IP Telephony Node: 1001 TPS Firmware
Update
Phone Type
TPS Firm
1 IP Audio Conference Phone 2033 Not Available S74
2 IP Phone 1110 C8A C6O
Recommended versions of the Set firmware is held in the Currency file. This cant currently be downloaded from the link arrowed below.
Go to Support.Avaya.com
Select DOWNLOADS and Comms Server 1000E for a copy
It is then selected and UPLOADed as shown below to the server.
Update Recommended Firmware List
You can download the latest recommended firmware list from the Avaya Support web site. Once downloaded, it can be uploaded to the Master TPS of this IP Telephony Node.
C:\Users\Phil\Desktop\F
Browse...
Only file name of currency.xml or file type of .zip is accepted.
Select Currency file.
346

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

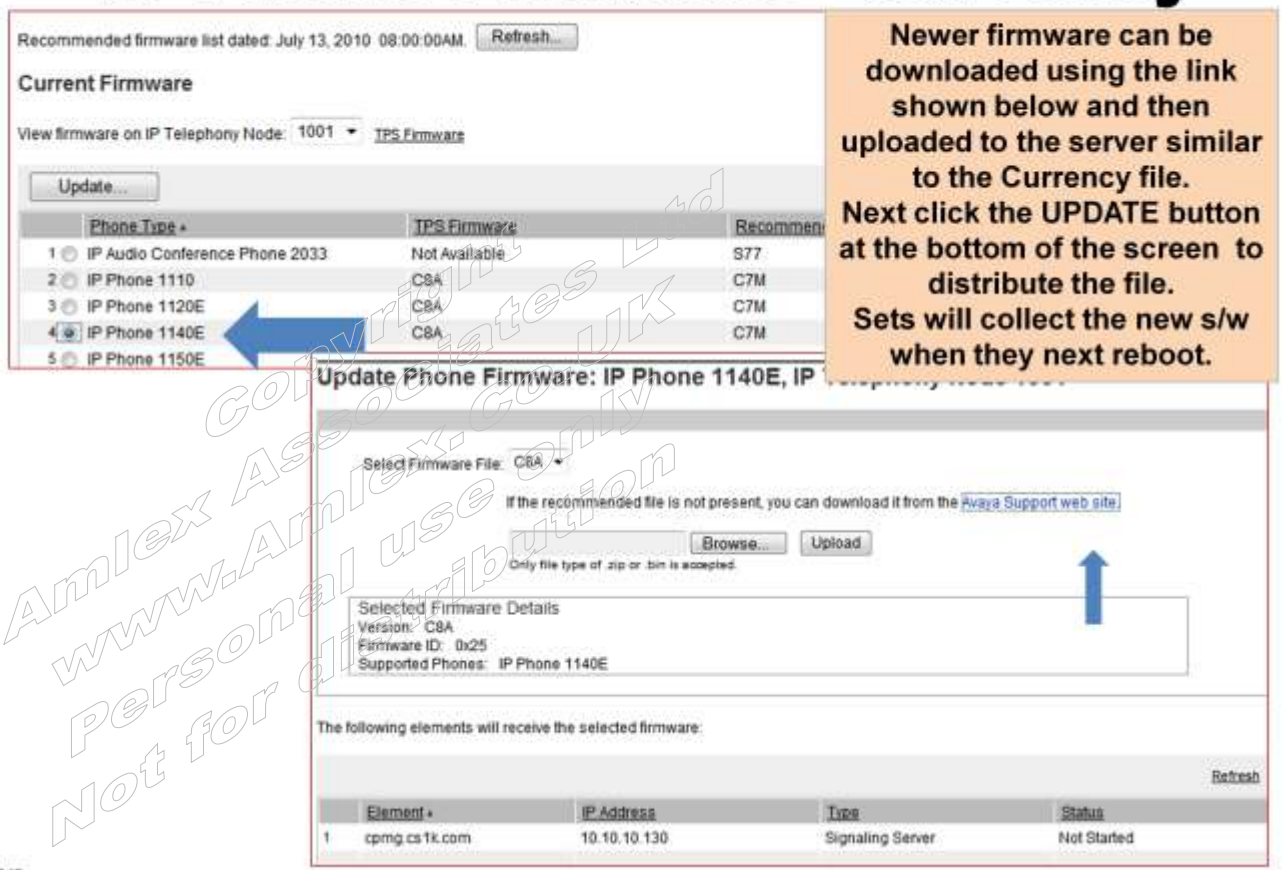
You can see from these slides that both the recommended list and the TPS Firmware for the Node has now been upgraded.

Using the Link arrowed on the lower screen you can automatically download the required Firmware for Uploading to your servers.

It is necessary to reset the IP phone to force it to upgrade the firmware it is using.

This can be done manually by restarting the set or remotely by using the isetReset command on the signalling server.

IP Phone Firmware - Currency


Recommended firmware list dated: July 13, 2010 08:00:00AM.
Refresh...
Current Firmware
View firmware on IP Telephony Node: 1001
TPS Firmware
Update...
Phone Type
TPS Firmware
1 IP Audio Conference Phone 2033 Not Available S77
2 IP Phone 1110 C8A C7M
3 IP Phone 1120E C8A C7M
4 IP Phone 1140E C8A C7M
5 IP Phone 1150E
Newer firmware can be downloaded using the link shown below and then uploaded to the server similar to the Currency file.
Next click the UPDATE button at the bottom of the screen to distribute the file.
Sets will collect the new s/w when they next reboot.
Update Phone Firmware: IP Phone 1140E, IP
Select Firmware File: C8A
If the recommended file is not present, you can download it from the Avaya Support web site.
Browse...
Upload
Only file type of .zip or .bin is accepted.
Selected Firmware Details
Version: C8A
Firmware ID: 0x25
Supported Phones: IP Phone 1140E
The following elements will receive the selected firmware:
Refresh
Element
IP Address
Type
Status
1 cpmg.cs1k.com 10.10.10.130 Signaling Server Not Started

347

Notes

_____

_____

_____

_____

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Troubleshooting IP sets

There are a few options to check sets from the Element Manager itself. One of these is a simple Ping from the Element Manager itself.

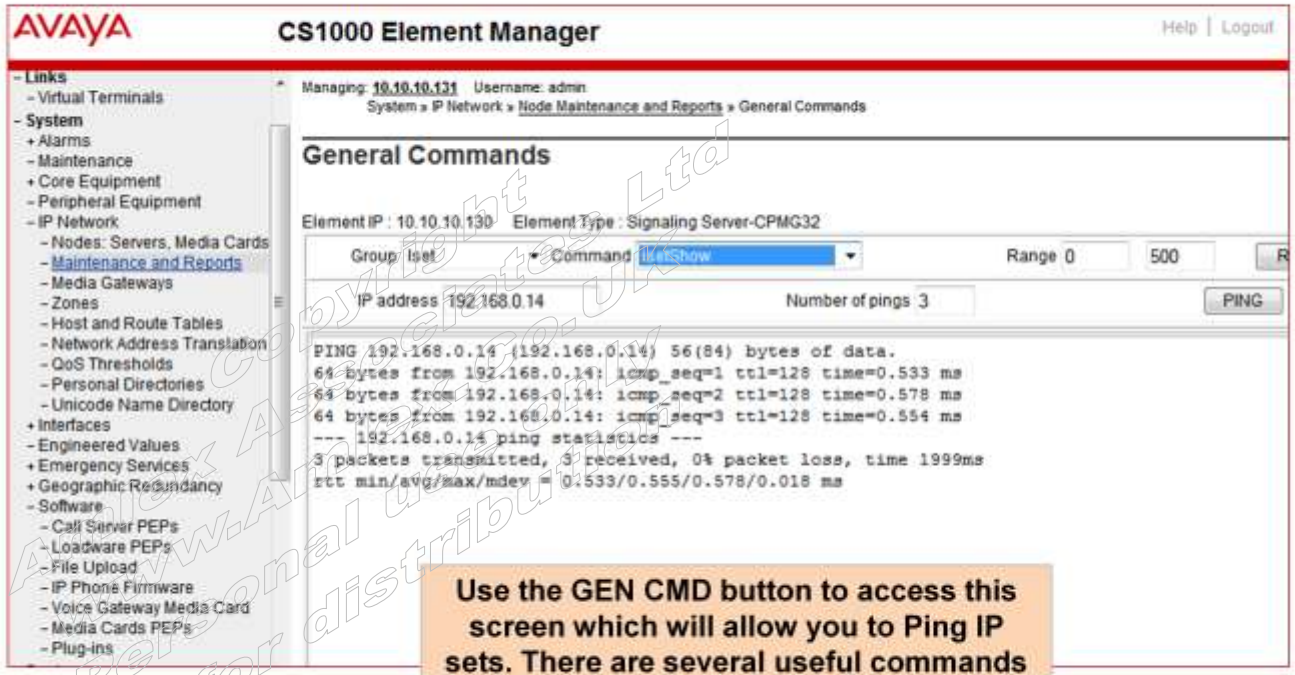
Select the IP NETWORK / MAINTENACE AND REPORTS menu option. This will display the screen we used to look at the Node logs.

On this screen select the GEN CMD button for one of the components and you will get a screen similar to that shown. Enter the IP address of the set and use the PING button to test connectivity.

There are several useful commands on this screen which are otherwise accessed from the command line of the Signalling Server.

Use the GROUP Drop-down Menu to select a command group then the COMMAND drop down for specific commands.

e.g. Group – Iset
Command – isetShow
Displays IP sets registered to the Sig Server.



348

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

IP Set Diagnostics

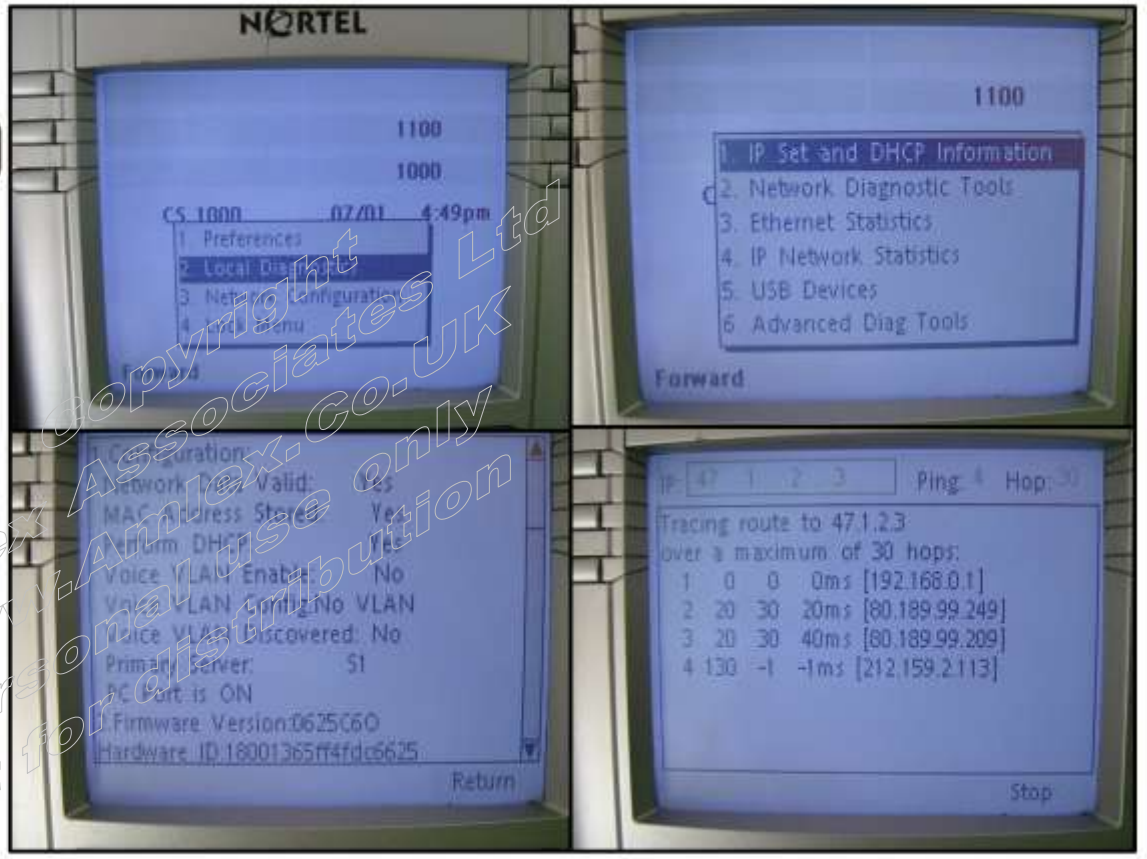
On the IP set itself you can perform several simple checks and Diagnostics.

Access the Local Tools menu by a swift double press on the services key (A Globe with two arrows). From there select Local Diagnostics which will offer you a selection of information and diagnostics.

In the figure you can see the configuration information displayed as well as a **TRACEROUTE** from the set itself.

Using **PING** and **TRACEROUTE** from the Set can help to resolve issues on the sets especially things like one way speech.

Services Key



Copyright Amlex Associates Ltd
www.i-Amlex.co.UK
Personal use only
Not for distribution

349

Notes

_____

_____

_____

_____

Tracking Calls

The TRAC command in LD 80 can be a very useful tool for investigating problems on the system.

The syntax of the command is :-
TRAC <Customer No.> <DN>

>ld 80
TRA000
.trac 0 1200
ACTIVE TN 000 0 02 00 IPMG 000 0
ORIG VTN 252 0 05 10 KEY 0 SCR
Or
TRAC <TN>
.trac 100 0 0 0
VTN 100 0 00 00
KEY 0 SCR MARP IDLE
KEY 1 SCR MARP IDLE
KEY 2 NUL IDLE

Enhanced Trace
Monitors a TN (up to 3) constantly whilst you remain in overlay 80.

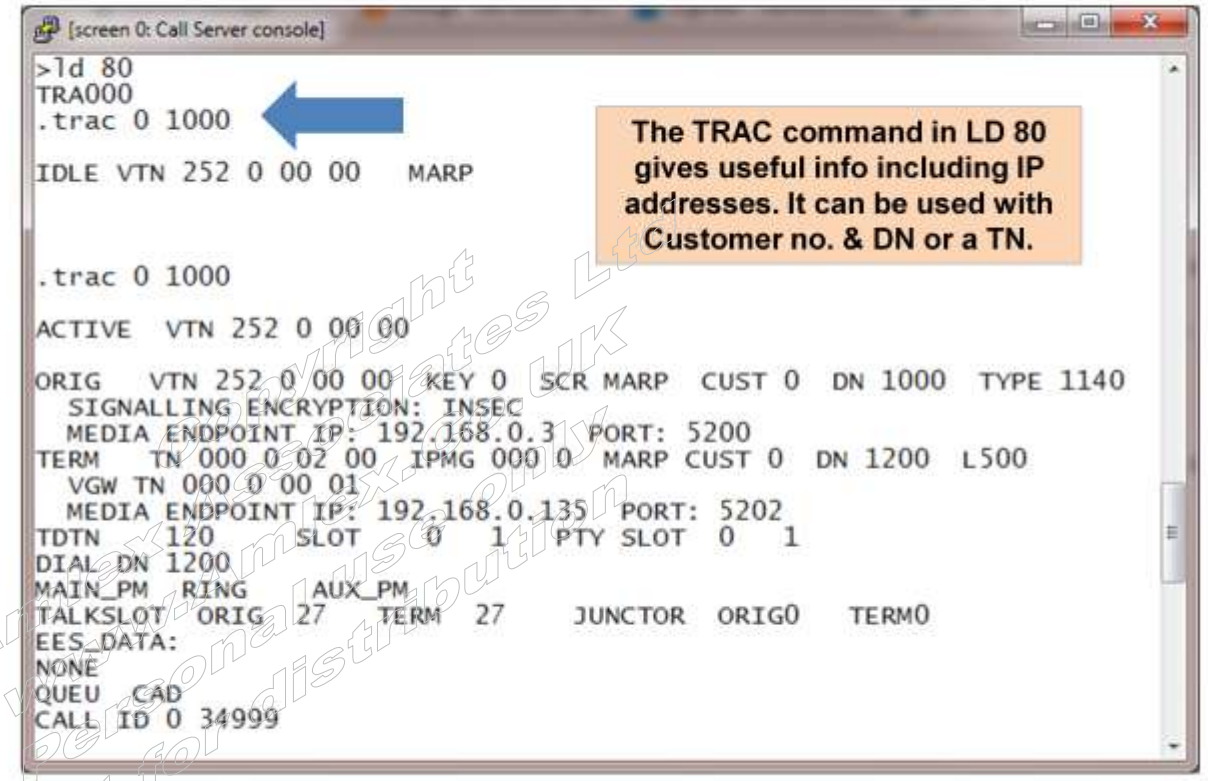
ENTC TN Time
Defines TN to trace & Time

eg >**ENTC 252 0 0 0 2300**

GOTR Starts the trace

FITR lists Hardware monitored

STPT Stop trace


[screen 0: Call Server console]
>ld 80
TRA000
.trac 0 1000
IDLE VTN 252 0 00 00 MARP
.trac 0 1000
ACTIVE VTN 252 0 00 00
ORIG VTN 252 0 00 00 KEY 0 SCR MARP CUST 0 DN 1000 TYPE 1140
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 192.168.0.3 PORT: 5200
TERM TN 000 0 02 00 IPMG 000 0 MARP CUST 0 DN 1200 L500
VGW TN 000 0 00 01
MEDIA ENDPOINT IP: 192.168.0.135 PORT: 5202
TDTN 120 SLOT 0 1 PTY SLOT 0 1
DIAL DN 1200
MAIN_PM RING AUX_PM
TALKSLOT ORIG 27 TERM 27 JUNCTOR ORIG0 TERM0
EES_DATA:
NONE
QUEU CAD
CALL ID 0 34999
The TRAC command in LD 80 gives useful info including IP addresses. It can be used with Customer no. & DN or a TN.

Amlex Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

350

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Monitoring the D-Channel is an extremely helpful tool in understanding what is happening to a routed call. However you need to be careful using this tool on a busy switch as it can generate a lot of output which could have an impact on performance.

The STAT MON command in LD 96 shown displays the current monitoring status. Monitoring is a two part operation as of Release 5:-

1. Enable the messages for DCH
2. Enable the output to either TTY a LOG file or both.

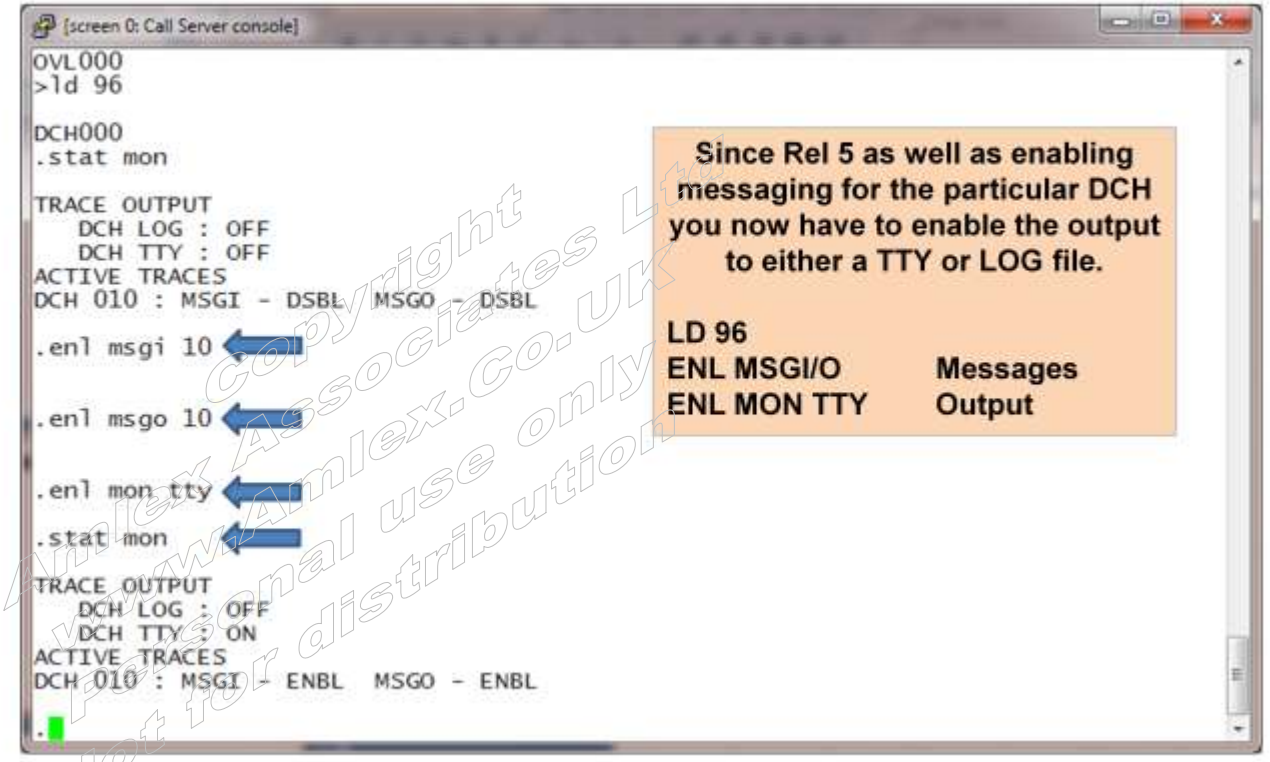
(In Previous Releases there was no option for the Trace Output)

To trace a D-Channel, firstly enable the inbound and/or outbound messages for the channel in question.

>enl msgi <DCH no.>

>enl msgo <DCH no.>

Monitoring D-Channel


[screen 0: Call Server console]
OVL000
>ld 96
DCH000
.stat mon
TRACE OUTPUT
DCH LOG : OFF
DCH TTY : OFF
ACTIVE TRACES
DCH 010 : MSGI - DSBL MSGO - DSBL
.enl msgi 10
.enl msgo 10
.enl mon tty
.stat mon
TRACE OUTPUT
DCH LOG : OFF
DCH TTY : ON
ACTIVE TRACES
DCH 010 : MSGI - ENBL MSGO - ENBL
.
Since Rel 5 as well as enabling messaging for the particular DCH you now have to enable the output to either a TTY or LOG file.
LD 96
ENL MSGI/O Messages
ENL MON TTY Output

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

351

Notes

_____

_____

_____

_____

D-Channel Output

Once the messages are turned on, you need to enable the output and this can be sent to either the TTY screen, a LOG file or both. This is also done in LD 96 :-

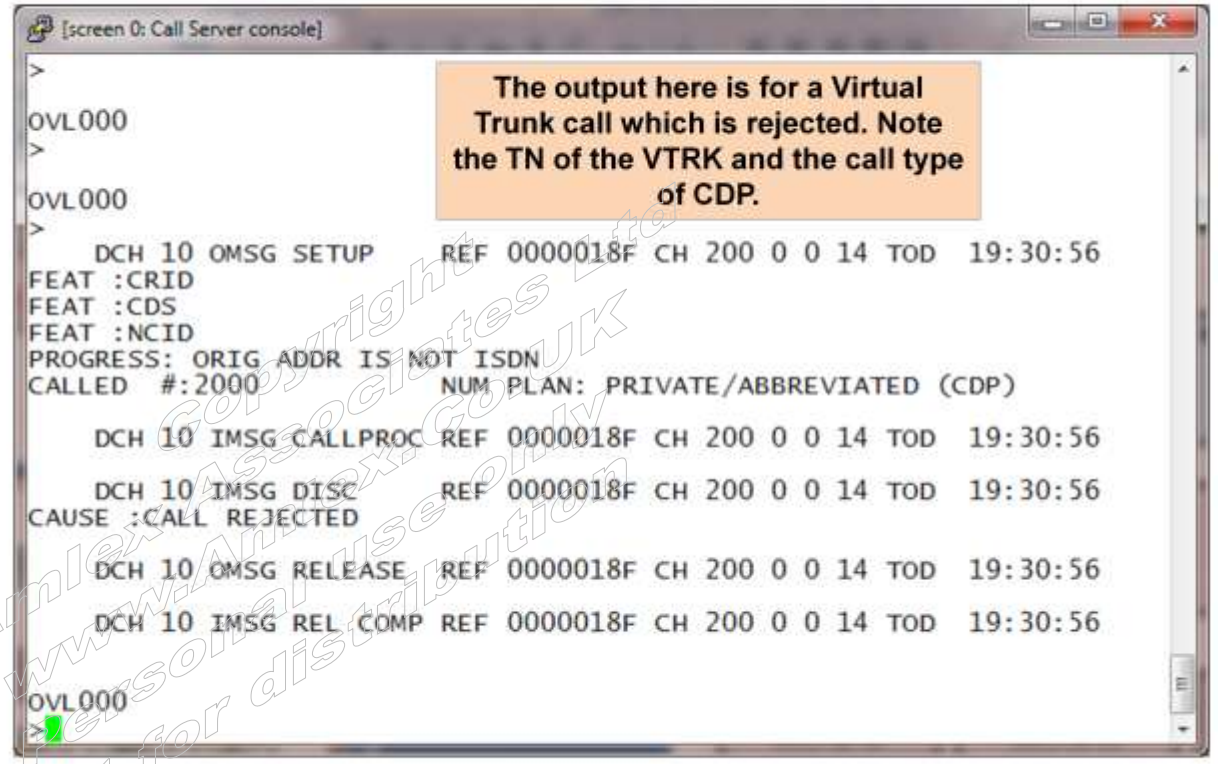
>enl mon tty **TTY**

>enl mon log **LOG file**

>enl mon all **TTY+LOG**

When using the log option the file is created in **/U/TRACE/DCH.LOG**.

The output shows a message sent out on TN 200 0 0 14 (A SIP virtual Trunk) from DCH 10, call type CDP. The inbound message shows a rejection and subsequent release of the channel.


[screen 0: Call Server console]
The output here is for a Virtual Trunk call which is rejected. Note the TN of the VTRK and the call type of CDP.
>
OVL000
>
OVL000
>
DCH 10 OMSG SETUP REF 0000018F CH 200 0 0 14 TOD 19:30:56
FEAT :CRID
FEAT :CDS
FEAT :NCID
PROGRESS: ORIG ADDR IS NOT ISDN
CALLED #:2000 NUM PLAN: PRIVATE/ABBREVIATED (CDP)
DCH 10 IMSG CALLPROC REF 0000018F CH 200 0 0 14 TOD 19:30:56
DCH 10 IMSG DISC REF 0000018F CH 200 0 0 14 TOD 19:30:56
CAUSE :CALL REJECTED
DCH 10 OMSG RELEASE REF 0000018F CH 200 0 0 14 TOD 19:30:56
DCH 10 IMSG REL COMP REF 0000018F CH 200 0 0 14 TOD 19:30:56
OVL000
>

Amlex Associates Ltd Copyright www.Amlex.co.UK Personal use only Not for distribution

352

16 April 2013

Notes

_____

_____

_____

_____

The SIP line gateway was introduced in Rel 6 but in Rel 7.5 it has been extended to embrace the Avaya One X Communicator.

The SIP line gateway resides on a Linux server and forms part of the IP telephony node. Sets communicate with the system using SIPL Virtual trunks and a special route configured purely for the purpose.

The UEXT allows the system to communicate more feature information to the sets than was previously possible allowing more features to be supported.

28. SIP Line Gateway

- SIP Line Gateway
  - Enables use of SIP Sets on CS1K
  - Part of IP Node
  - Uses UEXT to add features to SIP Phones
- Works alongside UniStim sets
  - Mixed Environment
- Avaya One X Communicator
  - Integrates with Avaya One X offering

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

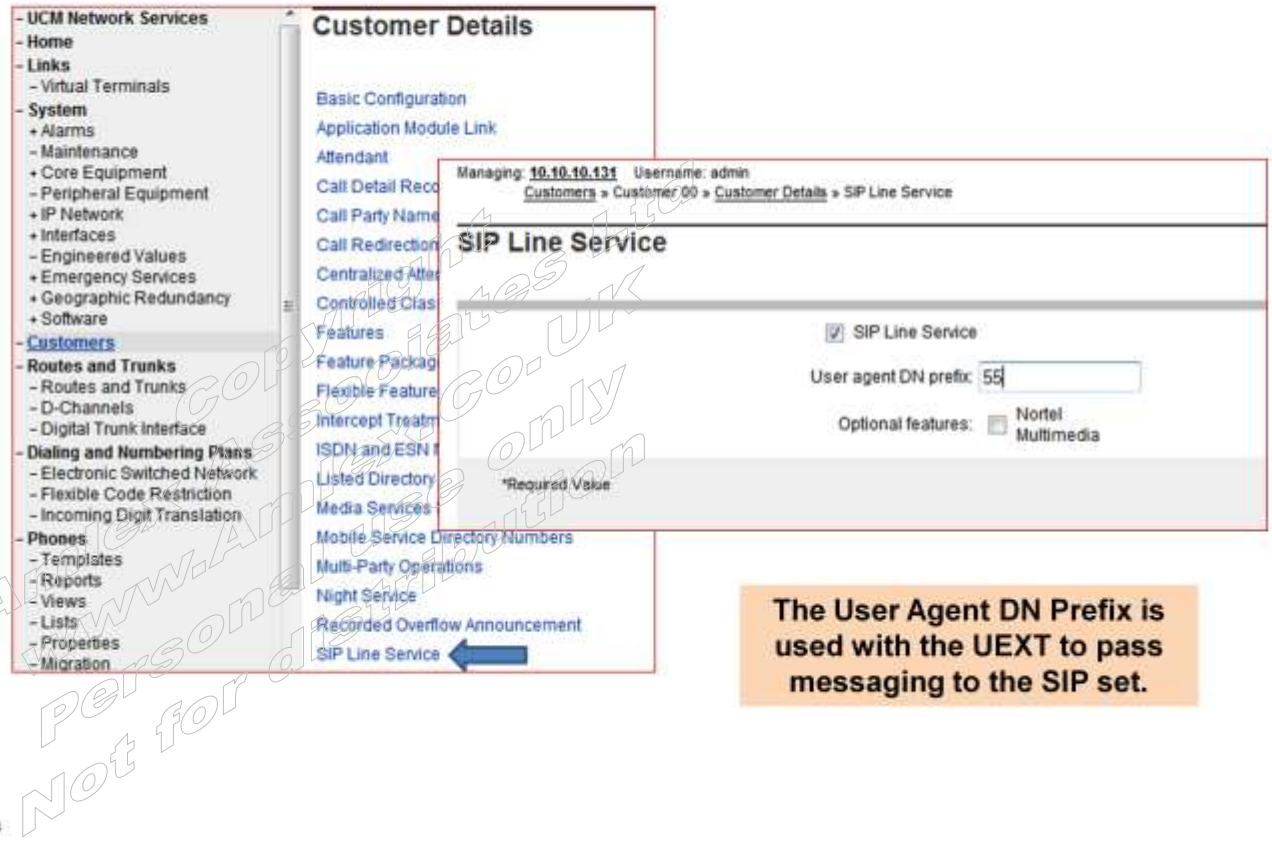
353

Notes

Enable SIP Line Service

To configure the SIP line gateway first you must enable it in the Customer area. Here you will also add a USER AGENT DN PREFIX this is used to identify the SIP sets along with the Primary DN assigned to them.

Here we have used the prefix 55.



Notes

_____

_____

_____

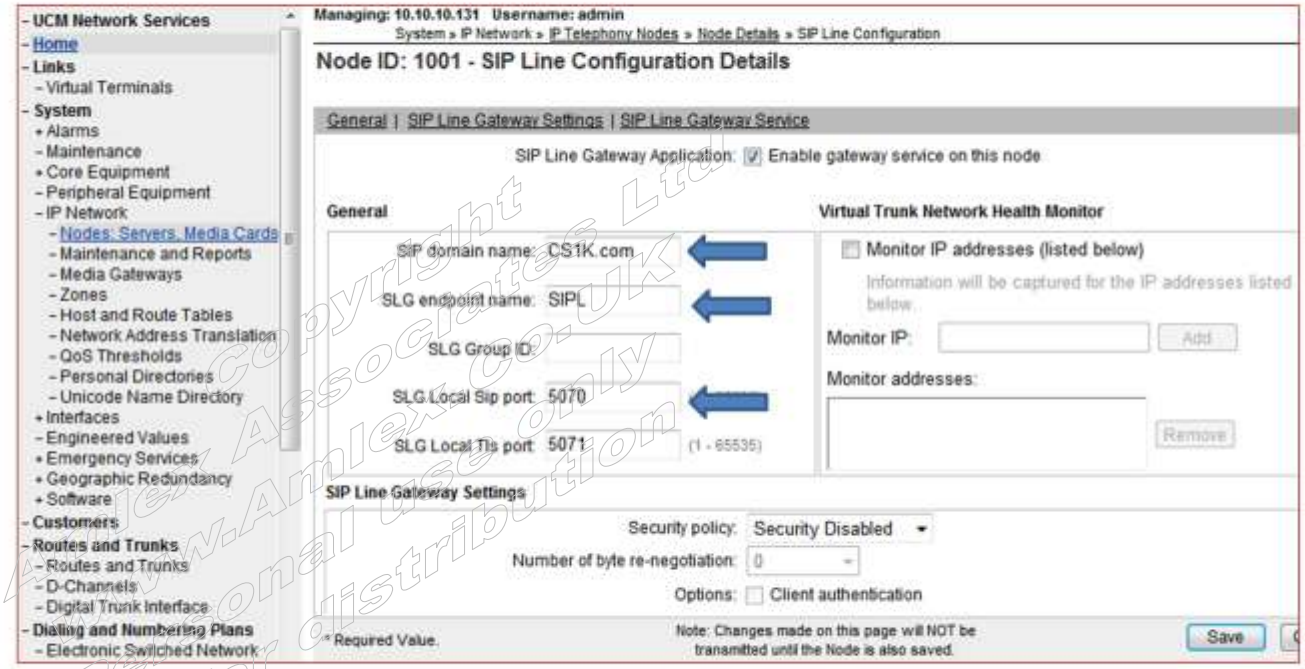
_____

Copyright Amlex Associates Ltd

Edit Telephony Node

The Telephony Node must be changed to add support for the SIP line Gateway. However if it is only being used for normal set registrations and not Branch Office or Geographic redundancy we only need to change the General settings as shown.

First add the SIP Domain as used for the existing Virtual Trunks. Then add an Endpoint name and set the SIP Port values as shown. We are using 5070 & 5071 as ports 5060 are in use for the SIP trunks.



Amlex Copyright Associates Ltd www.Amlex.co.uk Personal use only Not for distribution

355

Notes

_____

_____

_____

_____

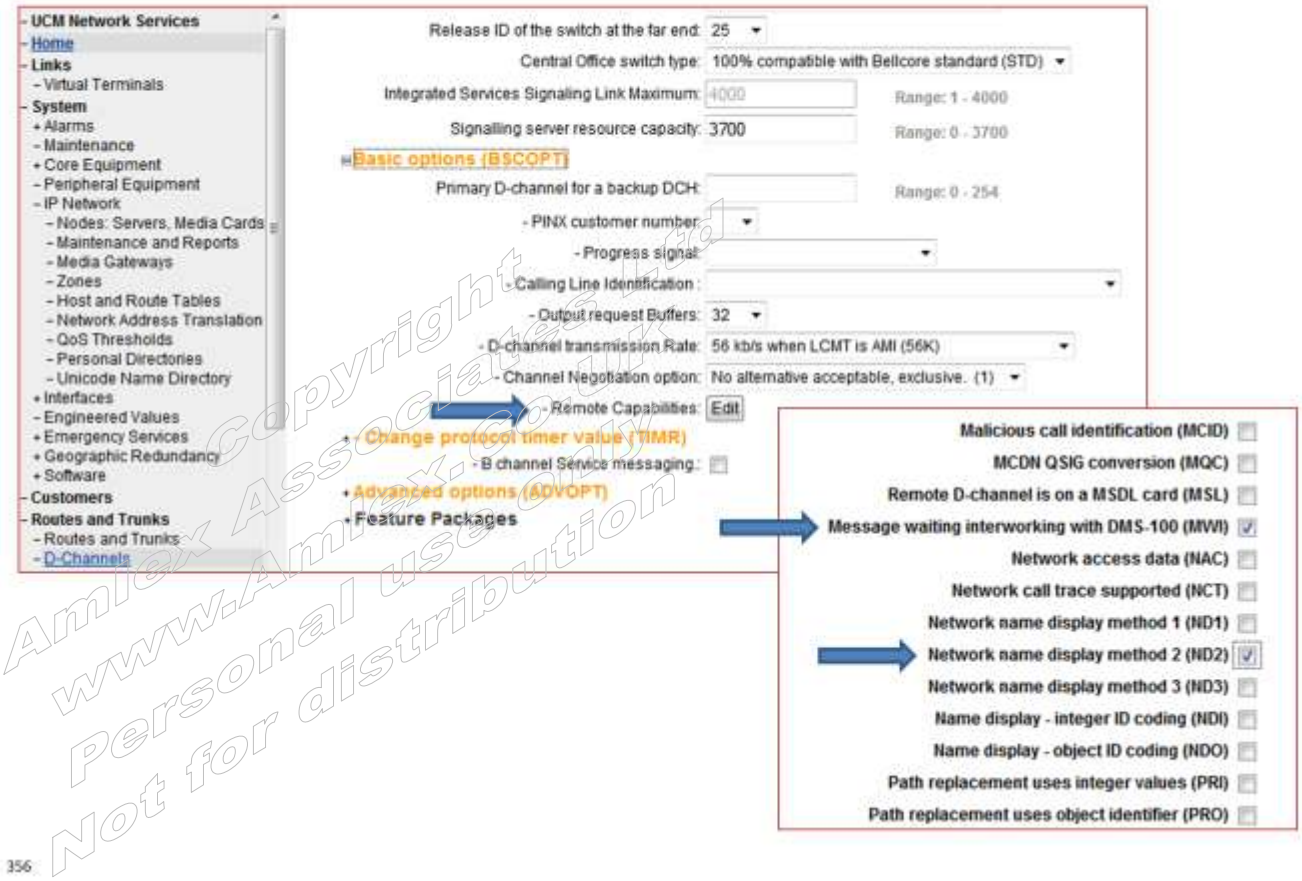
Copyright Amlex Associates Ltd

We can use the existing D Channel setup for the Virtual Trunks but we will need to add a couple of options to the Remote Capabilities.

First you will need to disable the D channel then edit the Remote Capabilities to add the Message Waiting option and Network name display.

Remember to enable the D channel again when you have added these options.

Edit D Channel


UCM Network Services
Home
Links
Virtual Terminals
System
Alarms
Maintenance
Core Equipment
Peripheral Equipment
IP Network
Nodes: Servers, Media Cards
Maintenance and Reports
Media Gateways
Zones
Host and Route Tables
Network Address Translation
QoS Thresholds
Personal Directories
Unicode Name Directory
Interfaces
Engineered Values
Emergency Services
Geographic Redundancy
Software
Customers
Routes and Trunks
Routes and Trunks
D-Channels
Release ID of the switch at the far end: 25
Central Office switch type: 100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000
Signalling server resource capacity: 3700 Range: 0 - 3700
Basic options (BSCOPT)
Primary D-channel for a backup DCH: Range: 0 - 254
PINX customer number:
Progress signal:
Calling Line Identification:
Output request Buffers: 32
D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)
Channel Negotiation option: No alternative acceptable, exclusive. (1)
Remote Capabilities: Edit
Change protocol timer value (TIMR)
B channel Service messaging:
Advanced options (ADVOPT)
Feature Packages
Malicious call identification (MCID)
MCDN QSIG conversion (MQC)
Remote D-channel is on a MSDL card (MSL)
Message waiting interworking with DMS-100 (MWI)
Network access data (NAC)
Network call trace supported (NCT)
Network name display method 1 (ND1)
Network name display method 2 (ND2)
Network name display method 3 (ND3)
Name display - integer ID coding (NDI)
Name display - object ID coding (NDO)
Path replacement uses integer values (PRI)
Path replacement uses object identifier (PRO)

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

356

Notes

_____

_____

_____

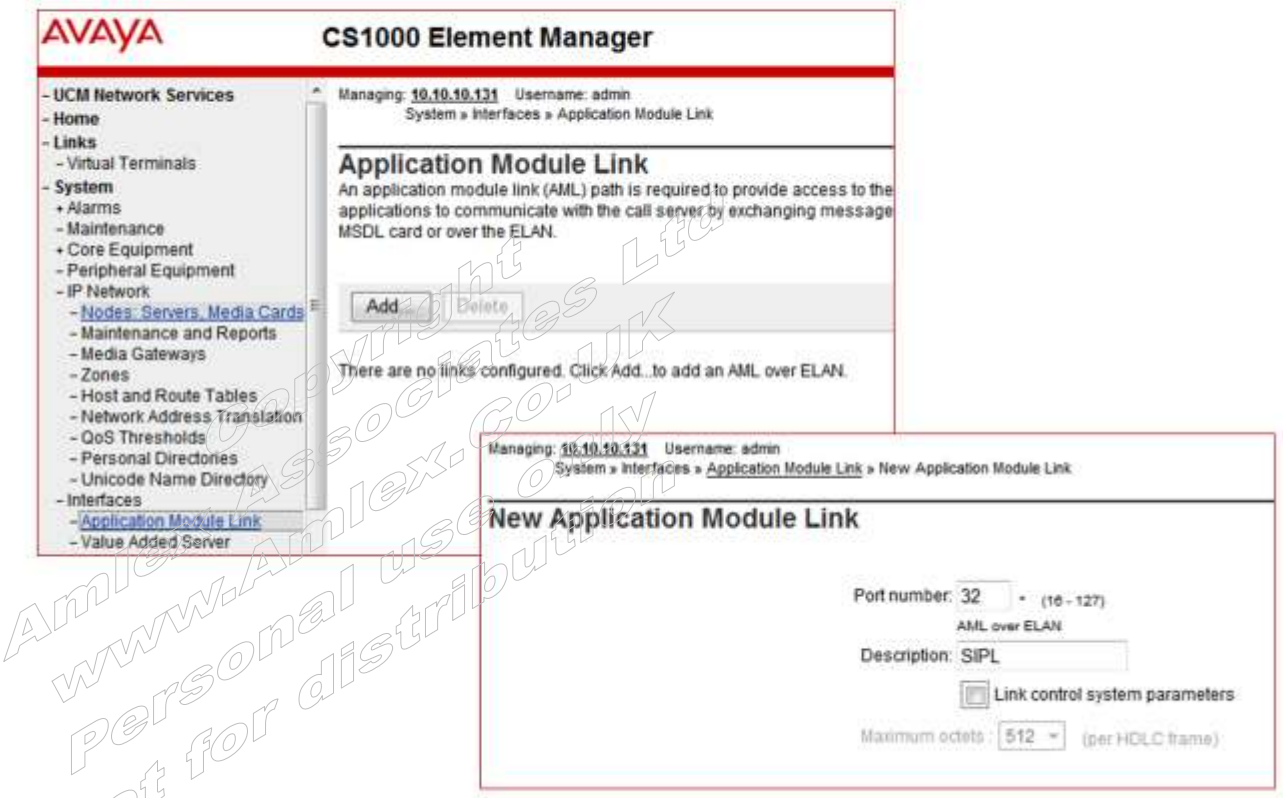
_____

Copyright Amlex Associates Ltd

Application Module Link

The next thing to configure is the Application Module Link which will be used to communicate with the SIP sets.

Add the Port number as shown and a description.


AVAYA
CS1000 Element Manager
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
- Interfaces
- Application Module Link
- Value Added Server
Managing: 10.10.10.131 Username: admin
System » Interfaces » Application Module Link
Application Module Link
An application module link (AML) path is required to provide access to the applications to communicate with the call server by exchanging message MSDL card or over the ELAN.
Add
There are no links configured. Click Add...to add an AML over ELAN.
Managing: 10.10.10.131 Username: admin
System » Interfaces » Application Module Link » New Application Module Link
New Application Module Link
Port number: 32 * (16 - 127)
AML over ELAN
Description: SIPL
Link control system parameters
Maximum octets: 512 (per HDLC frame)

357

Notes

_____

_____

_____

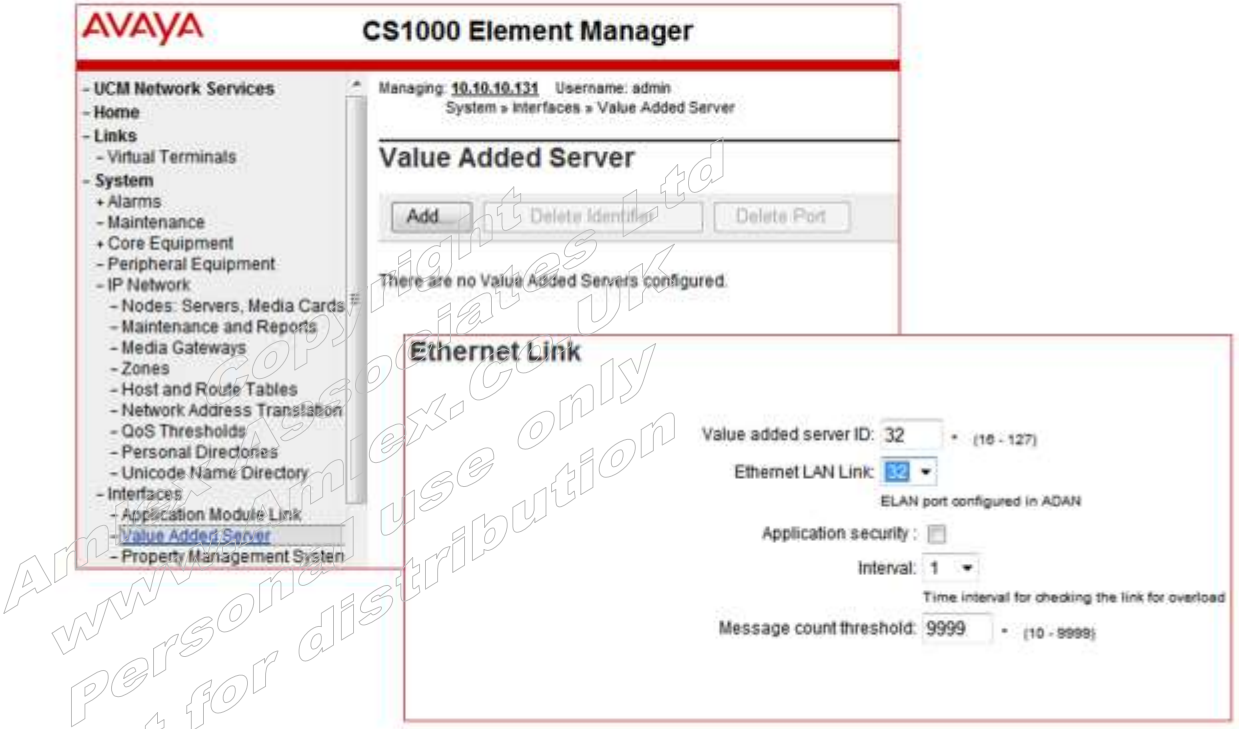
_____

Copyright Amlex Associates Ltd

Value Added Server

Along with the AML we need a Value Added Server. Select the VAS menu item and then select ETHERNET LINK.

The Server ID should match the Port number of the AML link and the Ethernet LAN link. Do not configure the Application Security .



Amlex Associates Ltd
www.amlex.co.uk
Copyright
Personal use only
Not for distribution

Notes

_____

_____

_____

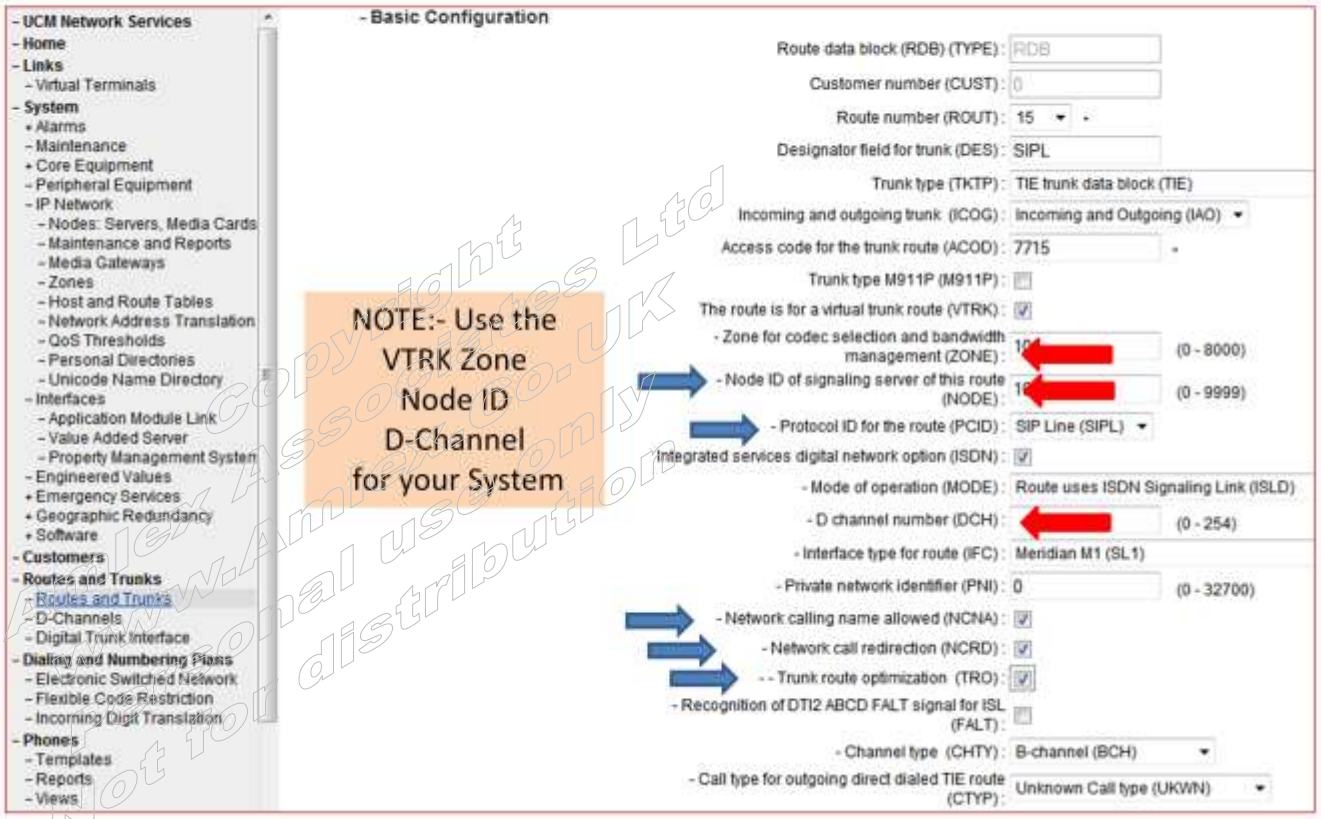
_____

Add SIP Line Route

With the AML and VAS configured we can move to configuring the new SIP route for the SIPL.

You may at this point want to add new Bandwidth zones for the SIP sets and the SIPL Virtual Trunks but it is possible to use the existing Zones for the UniStim sets.

The Node ID is set to the IP Telephony Node. The Protocol is set to SIPL and we need to check the three boxes shown NCNA, NCRD, and TRO.


- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
- IP Network
- Nodes: Servers, Media Cards
- Maintenance and Reports
- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
- Interfaces
- Application Module Link
- Value Added Server
- Property Management System
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 0
Route number (ROUT) : 15
Designator field for trunk (DES) : SIPL
Trunk type (TKTP) : TIE trunk data block (TIE)
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7715
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) :
(0 - 8000)
- Node ID of signaling server of this route (NODE) :
(0 - 9999)
- Protocol ID for the route (PCID) : SIP Line (SIPL)
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) :
(0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 0
(0 - 32700)
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- - Trunk route optimization (TRO) :
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)
NOTE:- Use the
VTRK Zone
Node ID
D-Channel
for your System
359

Notes

_____

_____

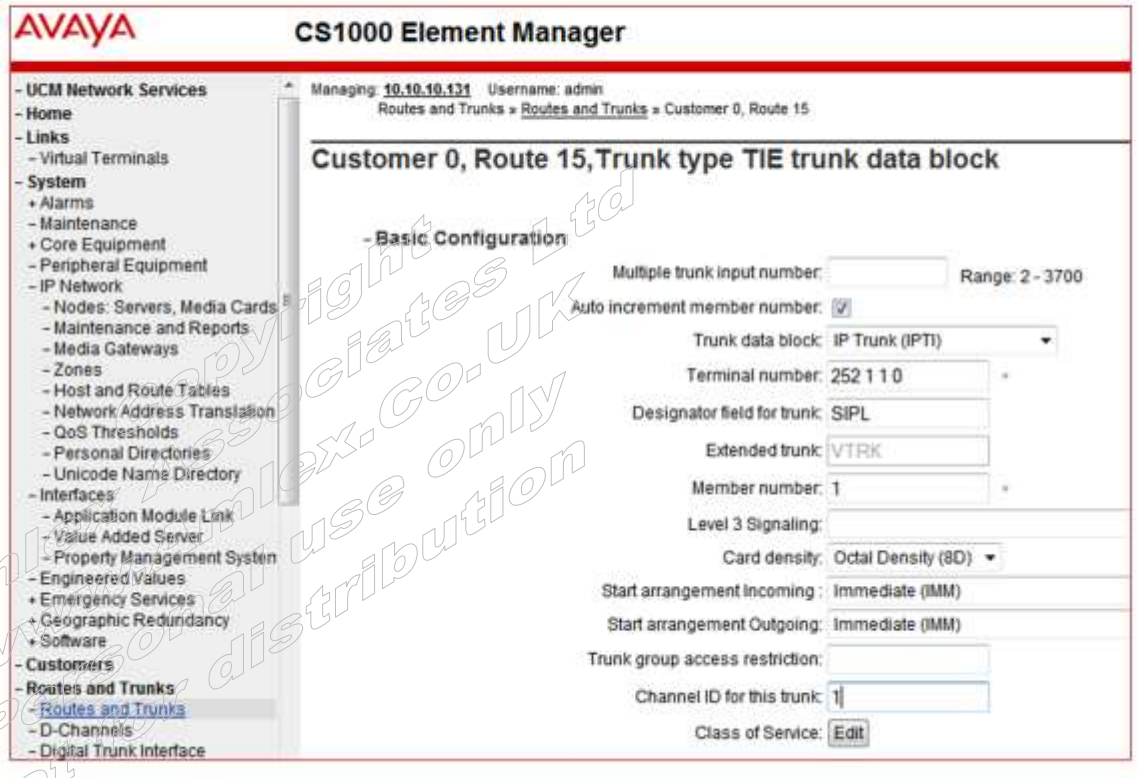
_____

_____

Copyright Amlex Associates Ltd

Add Trunks

With the Route in place the trunks can be added. Again these are very similar to the Virtual Trunks already configured.



Amlex Copyright
www.amlex.co.uk
Personal use only
Not for distribution

360

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

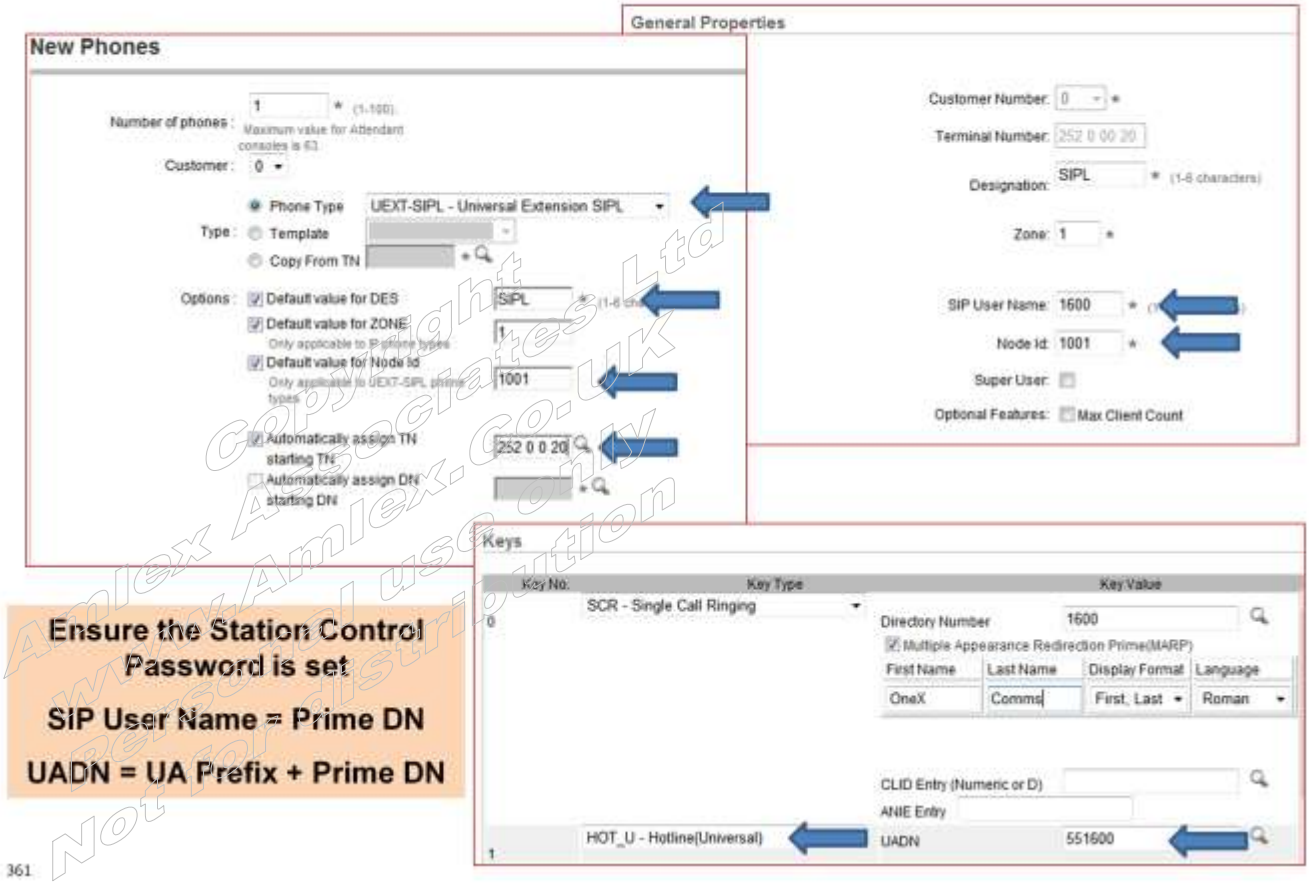
Add SIP Set

The SIP sets are added as UEXT-SIPL as shown here. You need to add the value for the Node ID as well as the Zone.

In the General Properties screen shown you should set the SIP User Name to the Prime DN of the set (i.e. Key 0).

In the Features section remember to assign SCPW a station control Password, you may need to set the length of SCPW before one can be entered. In addition you need to enable CNDA and DNDA, to allow names to be displayed.

Finally Key 0 is set with the Prime DN and Key 1 is set as a HOT_U (Hotline) with the UADN configured as the Prefix set earlier in the SIP Line Service, followed by the Prime DN.


New Phones
Number of phones: 1 (1-100)
Maximum value for Attendant consoles is 63
Customer: 0
Type: Phone Type UEXT-SIPL - Universal Extension SIPL
Template
Copy From TN
Options: Default value for DES SIPL
Default value for ZONE 1
Only applicable to IP phone types
Default value for Node Id 1001
Only applicable to UEXT-SIPL phone types
Automatically assign TN starting TN 252 0 0 20
Automatically assign DN starting DN
General Properties
Customer Number: 0
Terminal Number: 252 0 00 20
Designation: SIPL (1-8 characters)
Zone: 1
SIP User Name: 1600
Node Id: 1001
Super User:
Optional Features: Max Client Count
Keys
Key No. Key Type Key Value
0 SCR - Single Call Ringing
Directory Number 1600
Multiple Appearance Redirection Prime(MARP)
First Name Last Name Display Format Language
OneX Comms First, Last Roman
CLID Entry (Numeric or D)
ANIE Entry
1 HOT_U - Hotline(Universal)
UADN 551600
Ensure the Station Control Password is set
SIP User Name = Prime DN
UADN = UA Prefix + Prime DN
361

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Configure One X Communicator

Now we need to install the One X Communicator and set it up to connect to the call server. Make sure you install all three packages in the install package.

First start the X-Communicator and add the Domain and the Extension number and Station Control Password set for the extension. By default the Communicator will set the transport to TLS and we need to edit the config file to set this back to TCP.

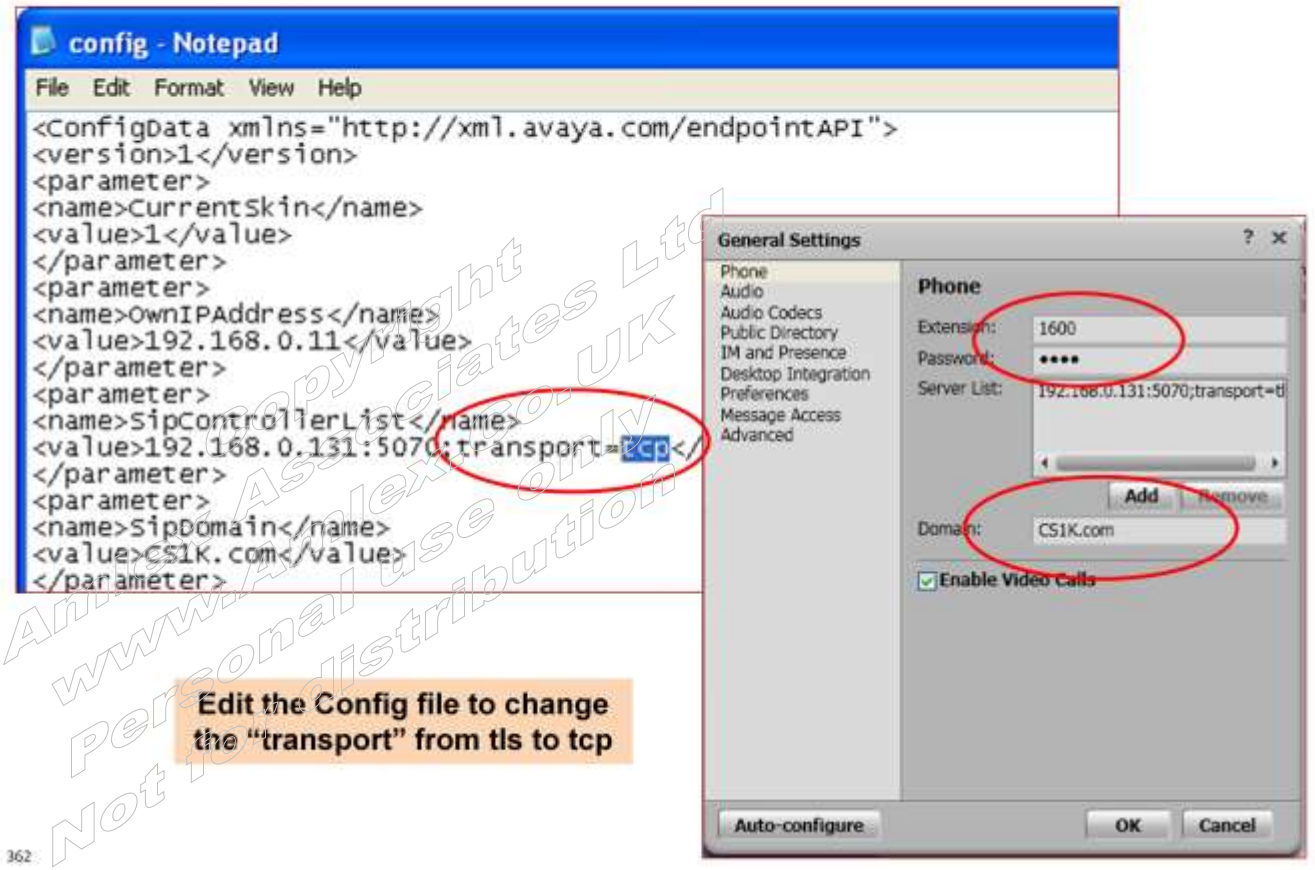
To do this shut down the programme and find the file config.xml in the directory :-
C:\Documents and Settings\<user>\Application Data\Avaya\Avaya one-X Communicator (Win XP)
or
C:\Users\<user>\AppData\Roaming\Avaya\Avaya one-X Communicator (Win 7).

NOTE:- you will probably have to view hidden files to find it.

Once opened with Notepad edit the line shown from :-

transport=tls to transport=tcp

Save the file and re-open One X Communicator.



Amlex Copyright www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

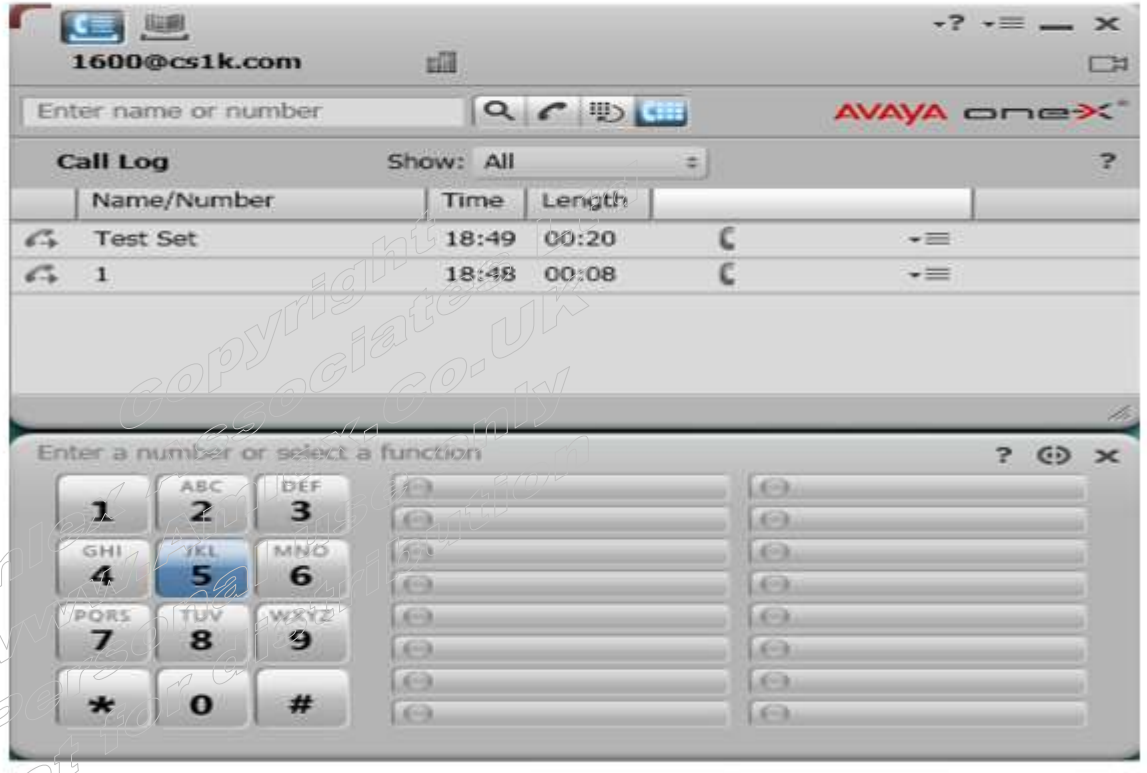
_____

Copyright Amlex Associates Ltd

One X Communicator

With the config file edited you should now be able to login to the call server correctly and call other extensions on the system.

Note the areas of the One X Communicator can be displayed or hidden and Un-docked from the main screen to suit the user.



363

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

There are three options for system redundancy.

Campus Redundancy is a single system whilst Branch office and Geographical redundancy are multi system configurations.

29. System Redundancy

- High Availability or Campus Redundancy
  - Dual Call Server
  - Resilience and Reduced Downtime
- Branch Office
  - For more remote locations
- Geographic Redundancy
  - Controlled Load Sharing
  - Survivable Media gateway

364

Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____
_____
_____
_____

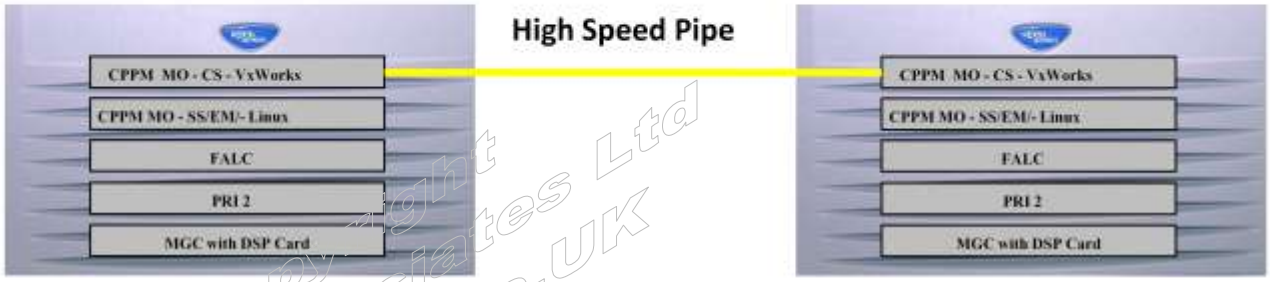
High Availability (HA) or Campus Redundancy is the Dual Processor option for the CS1K system. This option has been available on the "Big Switch" Meridian for many years and not only adds redundancy but also maintainability by allowing one side to be upgraded or repaired whilst the other continues giving service.

In the CS1K the option is available on both the CPPM cards as well as the Pentium IV for which it is the only configuration allowed.

The High Speed Pipe connection (Ethernet 1Gb) is used to maintain synchronisation of both the FMD and the memory between the two systems.

Package 410 must be included in the system software to allow HA operation.

High Availability – Campus Redundancy



- Dual Processors
  - Pentium IV or CPPM
  - VxWorks Only
  - High Speed Pipe to synchronise both CPU's
  - Package 410
- HSP can be extended using Fibre
  - Network must support
    - Round Trip Delay less than 30ms
    - Packet loss Less than 0.1%

365

Amlex Copyright www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

The Branch Media Gateway MG1000B or branch Office system is a separate call server offering system redundancy for IP sets only.

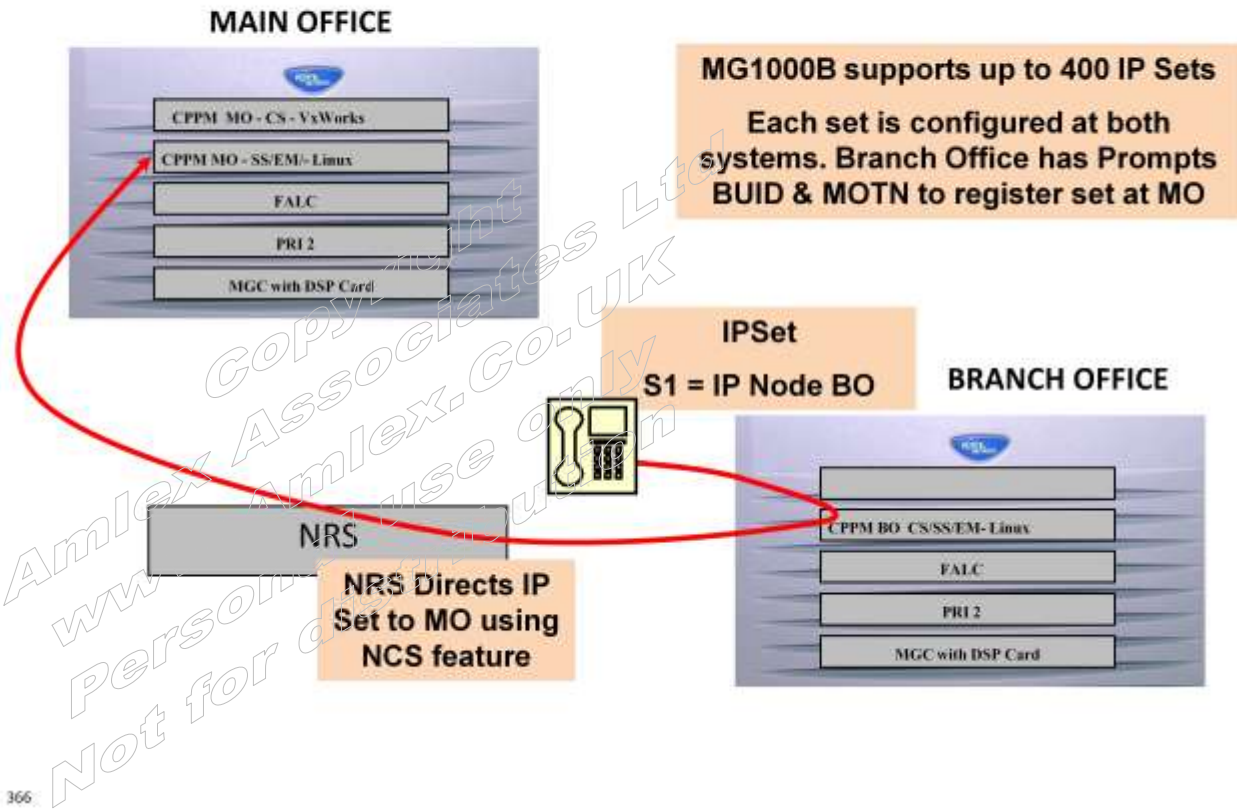
The Branch office system supports both IP sets and TDM resources but the IP sets are only registered to the system during a failure. IP sets can run in "Local" mode for up to 90 days.

The Branch office is a system in its own right and is configured separately from the main office communicating with it via IP Virtual trunks. IP sets must be configured on both the Main Office system where they are registered whilst in normal operation, known as "Normal" mode as well as at the Branch office.

On the Branch Office system it is the extra BUID (Branch User ID) and MOTN (Main Office TN) prompts which tell the IP set that it should re-register to the Main Office system. The main office is located using the NRS (NCS).

IP sets must be configured to register at the Branch Office (i.e. Redundant node) initially before being diverted to the Main office.

Branch Office


MAIN OFFICE
CPPM MO - CS - VxWorks
CPPM MO - SS/EM/- Linux
FALC
PRI 2
MGC with DSP Card
MG1000B supports up to 400 IP Sets
Each set is configured at both systems. Branch Office has Prompts BUID & MOTN to register set at MO
IPSet
S1 = IP Node BO
BRANCH OFFICE
NRS
NRS Directs IP Set to MO using NCS feature
CPPM BO CS/SS/EM- Linux
FALC
PRI 2
MGC with DSP Card
366

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

In the Controlled Load Sharing option each system is fully licensed and running in its own right.

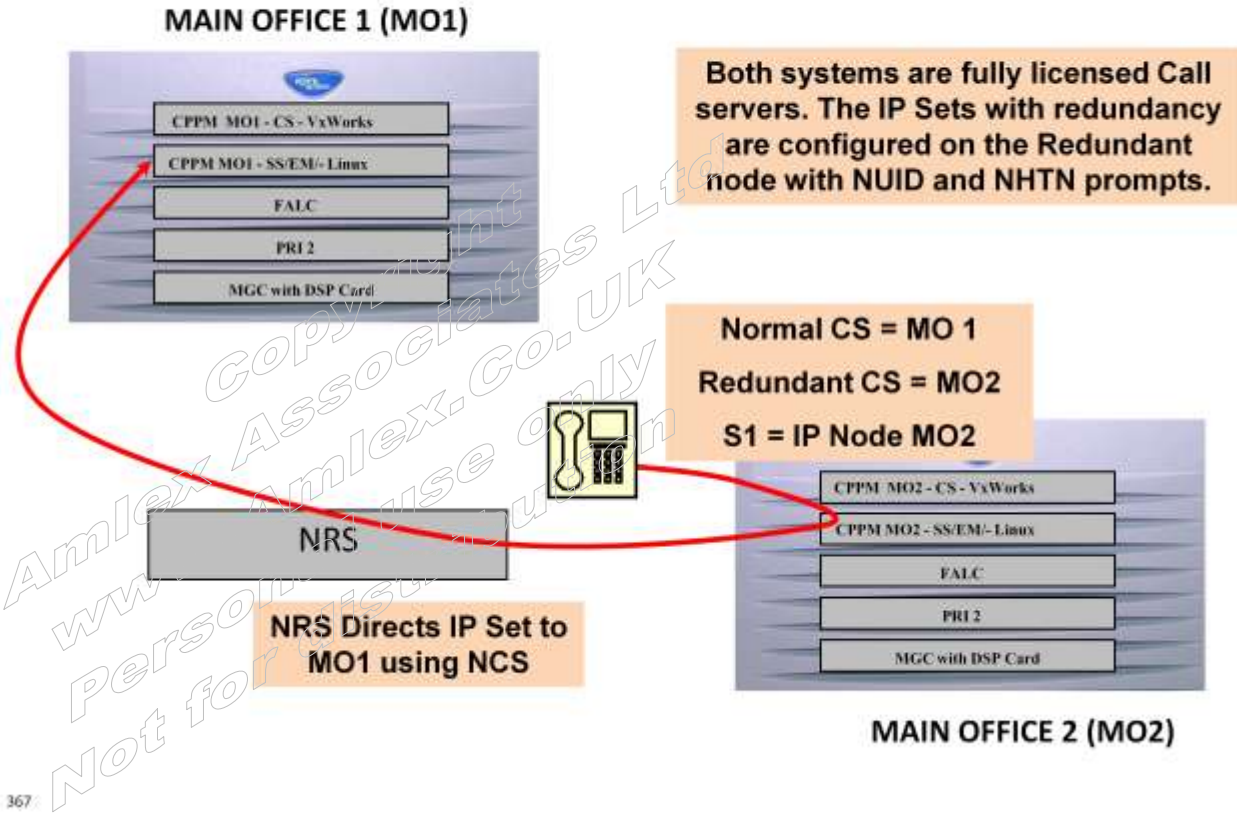
Where IP sets need to have redundancy they are configured on both systems in a similar fashion to the Branch office solution. However the two prompts which are now completed on the redundant node are NUID (Network User ID) and the NHTN (Network Home TN).

In a similar fashion to the Branch office the IP set registers momentarily to the redundant node and because the NUID and NHTN are configured it is sent to re-register on its home system. This is again found using the NCS component of the NRS.

Again IP sets must be configured to register at the alternate system (i.e. Redundant node) initially before being diverted to the Main office.

The Controlled Load Sharing option uses the Temporary License for IP sets which are to have redundancy. When the NUID and NHTN are configured for a set the system knows to use a Temporary (90 day) license rather than a full IP set license.

Controlled Load Sharing


MAIN OFFICE 1 (MO1)
CPPM MO1 - CS - VxWorks
CPPM MO1 - SS/EM/- Linux
FALC
PRI 2
MGC with DSP Card
Both systems are fully licensed Call servers. The IP Sets with redundancy are configured on the Redundant node with NUID and NHTN prompts.
Normal CS = MO 1
Redundant CS = MO2
S1 = IP Node MO2
NRS
NRS Directs IP Set to MO1 using NCS
CPPM MO2 - CS - VxWorks
CPPM MO2 - SS/EM/- Linux
FALC
PRI 2
MGC with DSP Card
MAIN OFFICE 2 (MO2)
367

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

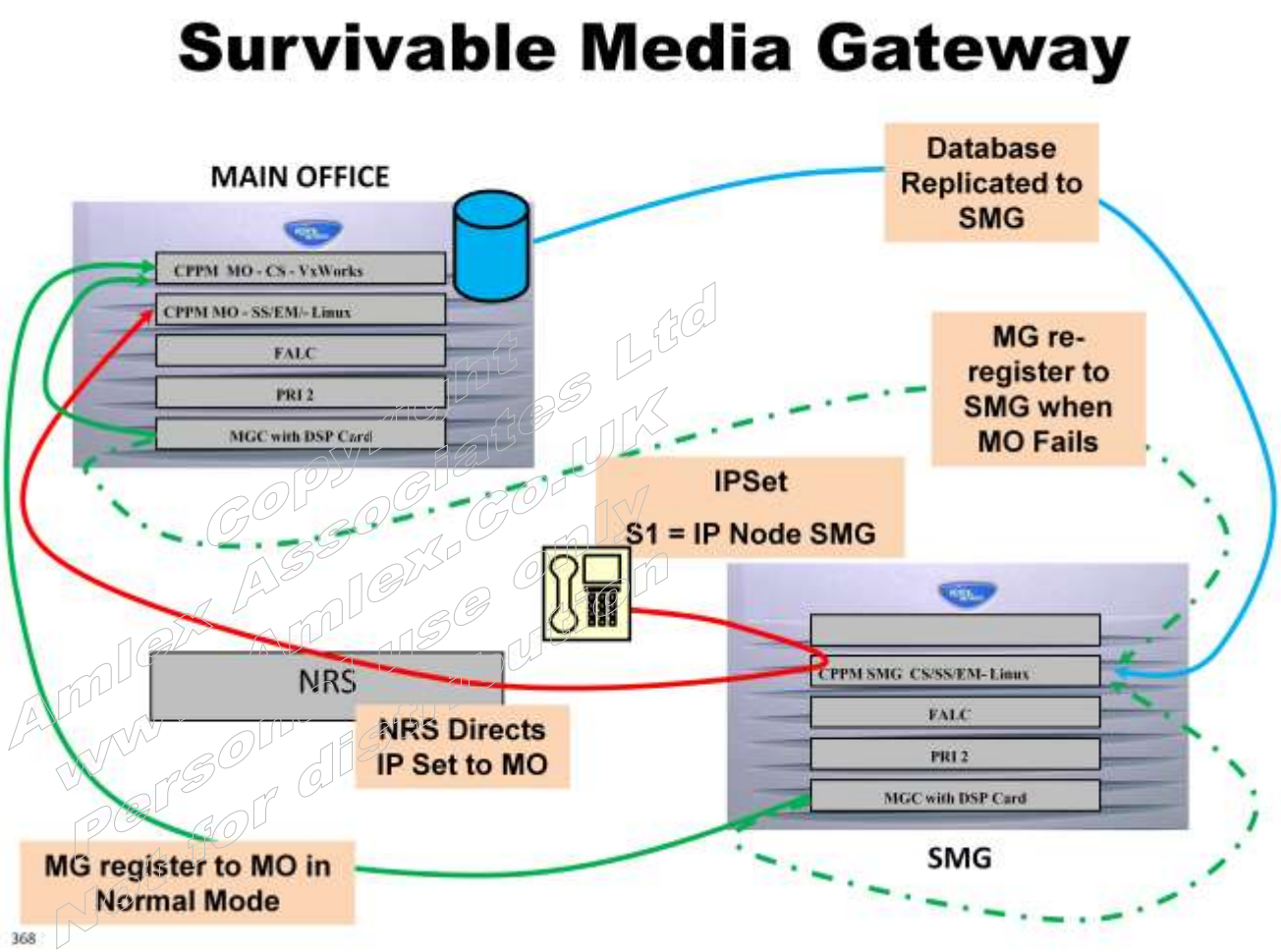
The Survivable Media Gateway (SMG) adds redundancy for both IP sets and Media gateways (and hence TDM resources) in the CS1K system. SMG's must be on a network with less that an 80ms round trip delay to the Call server and less than 0.05% packet loss.

Up to 50 media gateways can be defined on a Call server and in theory all of them can be configured with a survivable node.

In essence each SMG has a CS1K system of its own, i.e. a Call server (CS) and Sig Server (SS) so calls can continue to be processed. The SMG CS/SS unit is configured with a Node ID identical to the Main Office (MO) but of course the IP addressing will be different. The database from the MO is periodically copied to the SMG to keep it current.

In normal operation sets are configured (S1) to point to the redundant node where they momentarily register before being forwarded to the MO. Media Gateways also register to the MO.

When the MO is unavailable IP sets remain registered to the SMG and gain service from it. In addition the MGC's reboot and re-register to the SMG for service. This is known as Local Mode.



Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

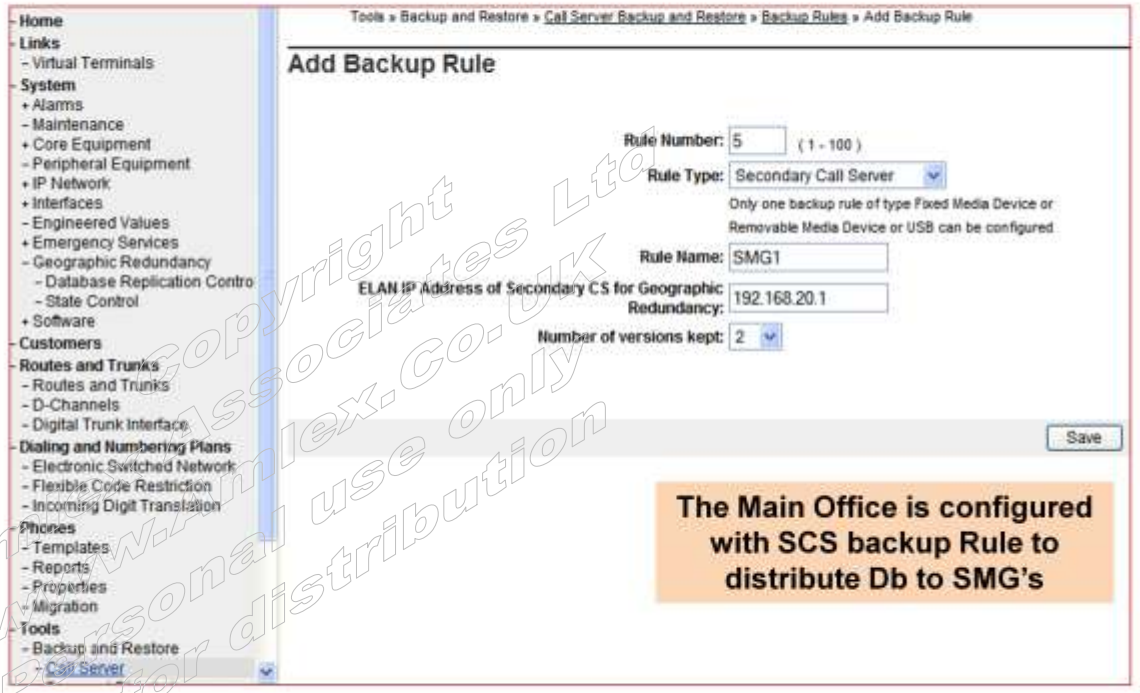
SMG – Backup Rule

To configure the system for a Survivable Media Gateway the Main Office is configured as normal.

The Survivable Media Gateway node (SMG) is installed as a normal call server and sig server except that a GRSEC keycode is installed. The IP Node for the SMG is configured with the same Node ID as the Main Office but IP addresses to suit its environment. The SMG requires only a basic database at this point as it will receive the MO database at a later stage.

The first addition to the MO is the Secondary Call Server (SCS) backup rule. This is specific for Geographic redundancy and sends a backup to another call server via FTP.

The configuration is shown here and the important element is the ELAN address of the Redundant (SMG) call server.


Home
Links
- Virtual Terminals
System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
- Geographic Redundancy
- Database Replication Contro
- State Control
+ Software
Customers
Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
Phones
- Templates
- Reports
- Properties
- Migration
Tools
- Backup and Restore
- Call Server
Tools » Backup and Restore » Call Server Backup and Restore » Backup Rules » Add Backup Rule
Add Backup Rule
Rule Number: 5 (1 - 100)
Rule Type: Secondary Call Server
Only one backup rule of type Fixed Media Device or Removable Media Device or USB can be configured
Rule Name: SMG1
ELAN IP Address of Secondary CS for Geographic Redundancy: 192.168.20.1
Number of versions kept: 2
Save
The Main Office is configured with SCS backup Rule to distribute Db to SMG's

Amlex Copyright
www.Amlex.Co.uk
Personal use only
Not for distribution

369

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Replication & State Control

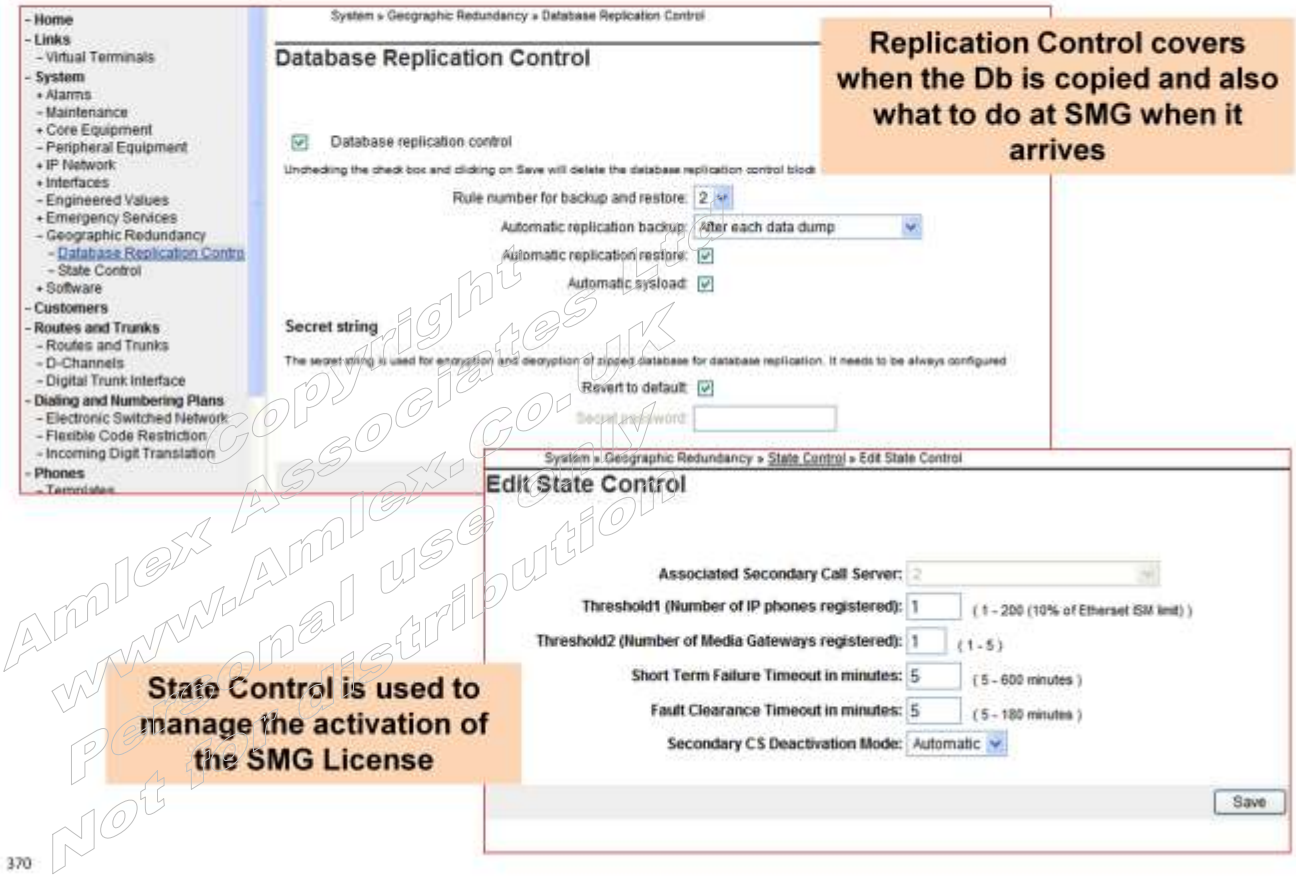
Once the SCS has been created the Replication Control can be configured as shown (Top). Here we define the Rule number that will be used and when the rule will be run.

In addition we need to check the boxes for Automatic Replication Restore and Automatic Sysload. These are actually used when the database is restored on the SMG to automatically bring it into service.

The State Control is also configured at this point which controls the activation of the GRSEC license on the SMG. Here you configure the number of IP sets and Media gateways registered that will bring the license to an active state.

In addition there are two timers that also control the transition from INACTIVE to ACTIVATING to ACTIVE and back to INACTIVE.

NOTE:-
Whilst we are configuring these on the MO it should be remembered that they will be used on the SMG to restore the database after replication.


- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
- Geographic Redundancy
- Database Replication Contro
- State Control
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
System » Geographic Redundancy » Database Replication Control
Database Replication Control
Database replication control
Unchecking the check box and clicking on Save will delete the database replication control block
Rule number for backup and restore: 2
Automatic replication backup: After each data dump
Automatic replication restore:
Automatic sysload:
Secret string
The secret string is used for encryption and decryption of zipped database for database replication. It needs to be always configured
Revert to default:
Secret password:
Replication Control covers when the Db is copied and also what to do at SMG when it arrives
System » Geographic Redundancy » State Control » Edit State Control
Edit State Control
Associated Secondary Call Server:
Threshold1 (Number of IP phones registered): 1 (1 - 200 (10% of Ethernet ISM limit))
Threshold2 (Number of Media Gateways registered): 1 (1 - 5)
Short Term Failure Timeout in minutes: 5 (5 - 600 minutes)
Fault Clearance Timeout in minutes: 5 (5 - 180 minutes)
Secondary CS Deactivation Mode: Automatic
Save
State Control is used to manage the activation of the SMG License
370

Amlex Associates Ltd Copyright
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Set a Location Code

The IP Sets will locate the MO using the NUID (Network User ID) & NHTN (Network Home TN) which are created automatically during database replication. This NUID is created from the AC code, Location code and user Extension. The Location is set as you can see here against the customer under the DPNSS option.

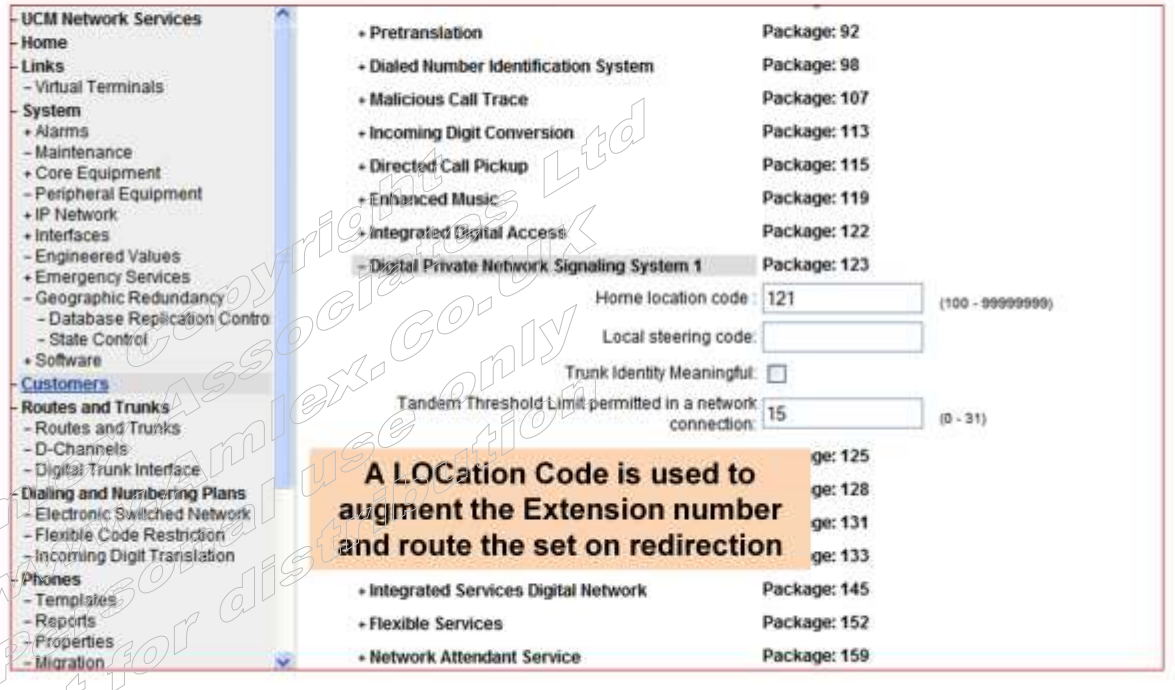
An example NUID would be :-

6 121 2000

and this will be seen on the IP set when it is registered to the main office in an SMG enabled system. The Set display will be :-

USER: 61212000

Because the sets need to use the NRS to locate the MO, it must also be setup with a route for this Location code.



371

Notes

_____

_____

_____

_____

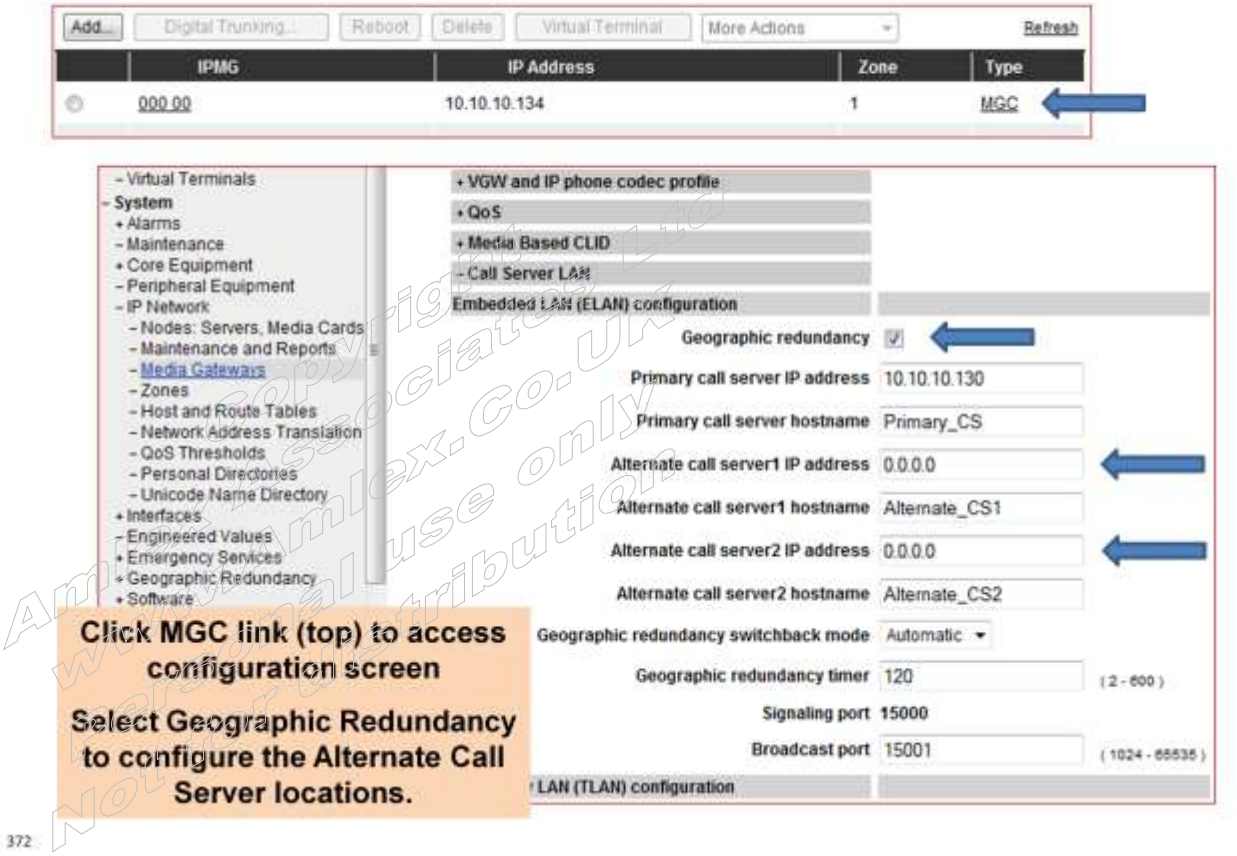
Copyright Amlex Associates Ltd

Media Gateway triple Registration

A call server configured for SMG operation has the benefit of Triple Registration for the Media Gateways themselves. This is done by adding up to two alternate Call server locations for each individual Media Gateway.

In the screenshot you will see that the GEOGRAPHIC REDUNDANCY option has been selected for the gateway which then adds the two alternate Call Server address fields. As this configuration is done on each media gateway individually, it is possible to group gateways together geographically around a survivable node.

When failure occurs the MGC will wait a preset time before rebooting and attempting to register with the next Call Server in the list.



Copyright Amlex Associates Ltd
www.amlex.co.uk
Not for external use only
No distribution

Notes

_____

_____

_____

_____

The SMG itself is installed as a normal Call Server / Sig Server system except with a GRSEC (Geographic Redundancy Secondary) license. This license gives up to 90 days continuous active usage.

The SMG can be a CoRes, SA or HA system depending on how many IP Sets and Media Gateways are to be supported.

Once the software is installed with a basic database the IP telephony node is configured with the same Node ID as the MO. In addition the Virtual Trunk gateways etc. should also be configured.

Once this is done the SCS backup rule , GR Replication Control and GR State control are all configured to match the settings on the MO. This is done to allow the first replication of the MO database.

Note:-
Once the first replication has taken place the Database on the SMG will be exactly the same as the one on the MO.

SMG Setup

- Install Software as normal
  - CoRes or separate CS & SS
  - Install a basic database
- Configure IP addresses and IP Node
  - IP Node has same ID number
  - Configure SIP/H323/NCS as necessary
- Configure – Same as on Main Office
  - SCS Backup Rule
  - GR Replication Control
  - GR State Control

Amlex Associates Ltd www.Amlex.co.uk Personal use only Not for distribution Copyright

373

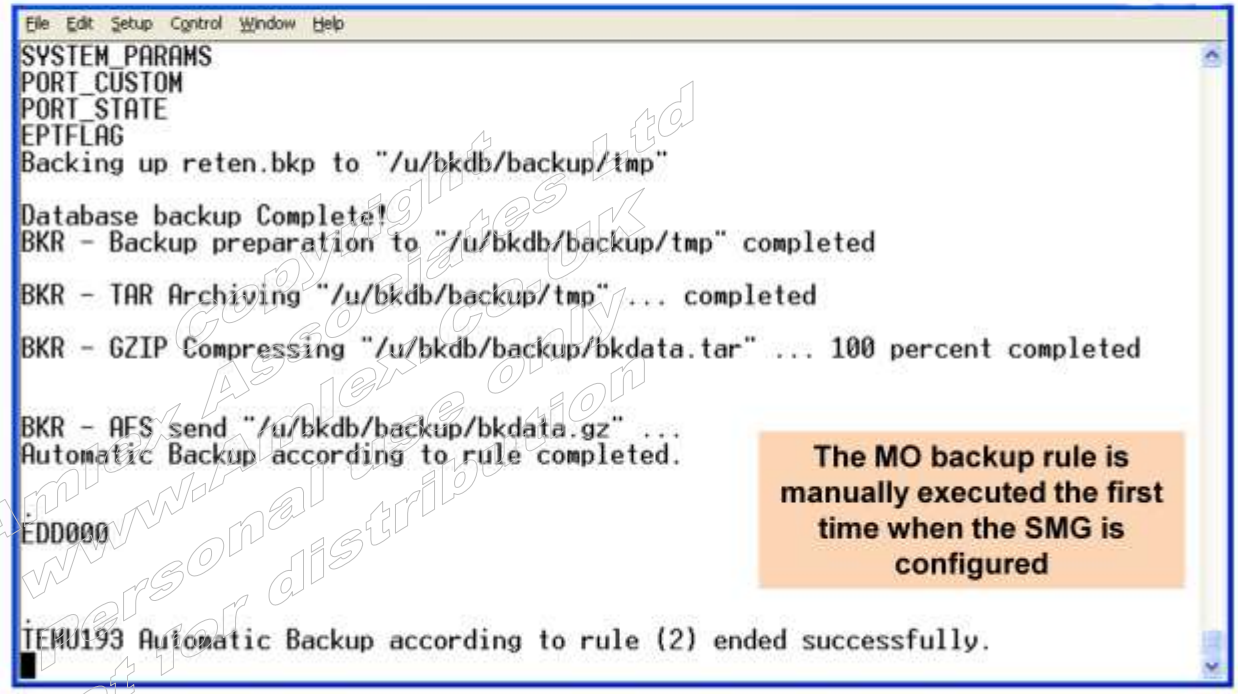
Notes

_____
_____
_____
_____

Backup using SCS Rule 1st time

Its important that the first Replication runs correctly as it sets up the system for future replications.

When the rule is run it backs up the system compresses the files (TAR & GUNZIP) and then copies the backup to the SMG Call Server.


File Edit Setup Control Window Help
SYSTEM_PARAMS
PORT_CUSTOM
PORT_STATE
EPTFLAG
Backing up reten.bkp to "/u/bkdb/backup/tmp"
Database backup Complete!
BKR - Backup preparation to "/u/bkdb/backup/tmp" completed
BKR - TAR Archiving "/u/bkdb/backup/tmp"... completed
BKR - GZIP Compressing "/u/bkdb/backup/bkdata.tar" ... 100 percent completed
BKR - AFS send "/u/bkdb/backup/bkdata.gz" ...
Automatic Backup according to rule completed.
EDD000
TEMU193 Automatic Backup according to rule (2) ended successfully.
The MO backup rule is manually executed the first time when the SMG is configured

374

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Restore to SMG 1st Time

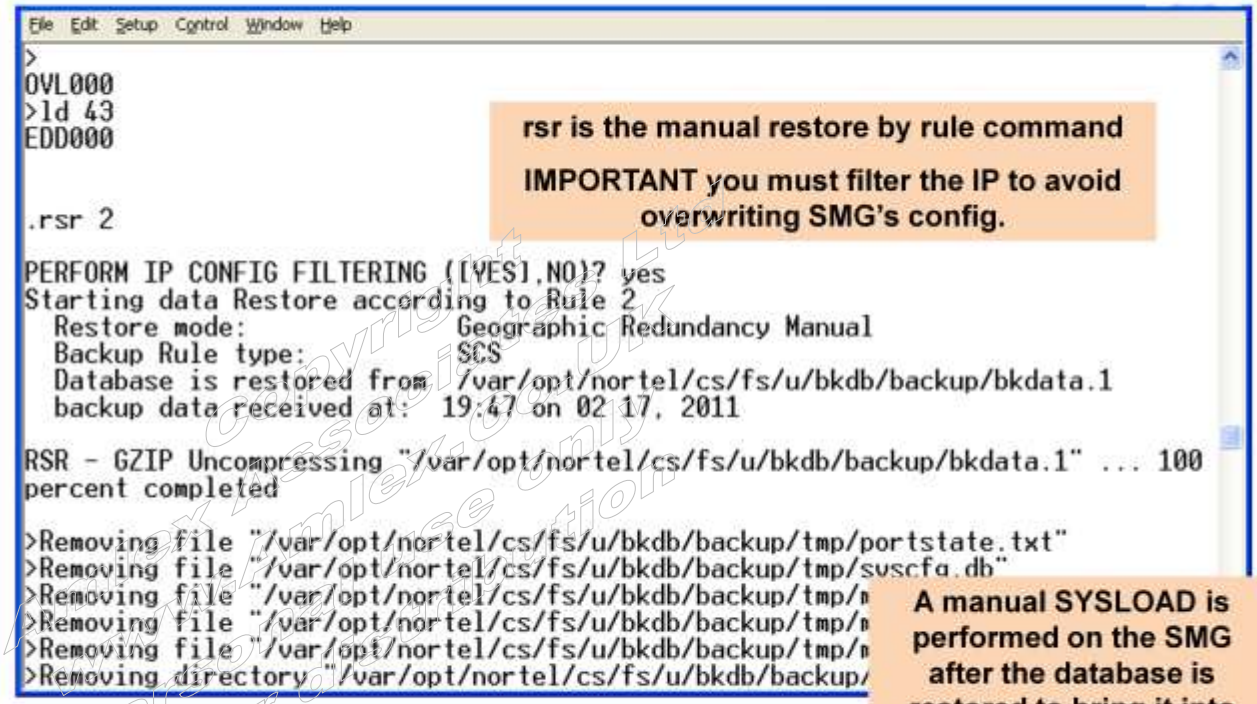
Because on the SMG we have not yet got a copy of the full database we need to manually run the backup rule to restore the database received and then manually Sysload the call server to bring it into service.

The command to run the restore by a rule is **RSR <Rule No.>** in LD 43.

The Sysload can be performed from LD 135 using the command **SYSLOAD ACTIVE .**

Once the Sysload has been performed you should have a copy of the MO database on the SMG.

If required add back the ELAN IP addresses of the Media gateways in LD 97.


File Edit Setup Control Window Help
>
OVL000
>ld 43
EDD000
.rsr 2
PERFORM IP CONFIG FILTERING ([YES],NO)? yes
Starting data Restore according to Rule 2
Restore mode: Geographic Redundancy Manual
Backup Rule type: SCS
Database is restored from /var/opt/nortel/cs/fs/u/bkdb/backup/bkdata.1
backup data received at: 19:47 on 02 17, 2011
RSR - GZIP Uncompressing "/var/opt/nortel/cs/fs/u/bkdb/backup/bkdata.1" ... 100 percent completed
>Removing file "/var/opt/nortel/cs/fs/u/bkdb/backup/tmp/portstate.txt"
>Removing file "/var/opt/nortel/cs/fs/u/bkdb/backup/tmp/sysctg.db"
>Removing directory "/var/opt/nortel/cs/fs/u/bkdb/backup/
rsr is the manual restore by rule command
IMPORTANT you must filter the IP to avoid overwriting SMG's config.
A manual SYSLOAD is performed on the SMG after the database is restored to bring it into service
LD 135 SYSLOAD ACTIVE

375

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

NRS Settings for SMG

As mentioned earlier we need the NRS to redirect the IP sets to the MO during registration.

Thus we need both the MO and SMG configured as endpoints on the NRS. Also the endpoint must be configured with Network Connection Service (NCS) support.

Having the SMG registered with the NRS will also allow us to continue using Virtual Trunks via the NRS when the MO has failed.

Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

376

Notes

_____

_____

_____

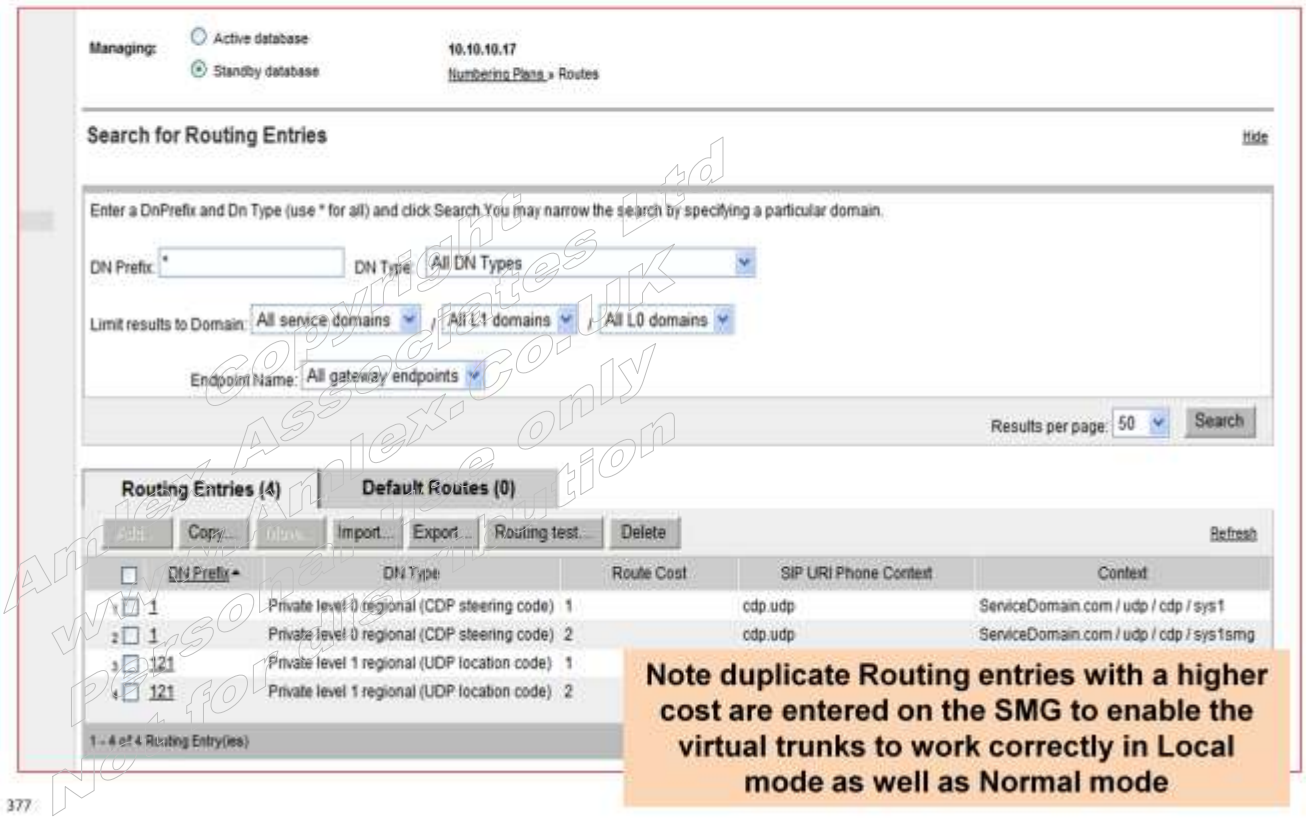
_____

Routing Entries

The endpoints will both need to be configured with both CDP and UDP routes to allow calls to be made and for the set registration redirection.

In the example you can see that we have the LOC configured as a UDP routing entry. This allows the IP sets to redirect correctly to the MO.

The entries on the SMG are both set with a route cost of 2 so that they will only be used when the primary route to the MO is not available. In this way the Virtual Trunks will continue to function correctly during the MO failure.


Managing:
Active database
Standby database
10.10.10.17
Numbering Plans » Routes
Search for Routing Entries
Hide
Enter a DnPrefix and Dn Type (use * for all) and click Search.You may narrow the search by specifying a particular domain.
DN Prefix: *
DN Type: All DN Types
Limit results to Domain: All service domains / All L1 domains / All L0 domains
Endpoint Name: All gateway endpoints
Results per page: 50
Search
Routing Entries (4)
Default Routes (0)
Add... Copy... Move... Import... Export... Routing test... Delete
Refresh
DN Prefix
DN Type
Route Cost
SIP URI Phone Context
Context
1 Private level 0 regional (CDP steering code) 1 cdp.udp ServiceDomain.com / udp / cdp / sys1
1 Private level 0 regional (CDP steering code) 2 cdp.udp ServiceDomain.com / udp / cdp / sys1smg
121 Private level 1 regional (UDP location code) 1
121 Private level 1 regional (UDP location code) 2
1 - 4 of 4 Routing Entry(ies)
Note duplicate Routing entries with a higher cost are entered on the SMG to enable the virtual trunks to work correctly in Local mode as well as Normal mode

377

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

The IP sets will be configured with their S1 setting pointing to the Node IP address of the redundant node i.e. the SMG. Thus the sets will momentarily register on the SMG before being redirected (Using the LOC & Extn NUID) to the MO via the NRS.

When sets are in Normal mode their displays will read as shown :-

USER:XYYYEXTN

To test the Local Mode operation use the Services Key on the set and select the **TEST LOCAL MODE** option. The set will register to the SMG.

To test the SMG operation try disabling the ELAN of the MO Call (SA only as HA will just swap sides).

In LD 135 use STAT GR on both MO and SMG to see the status of the licenses and the numbers of sets and media gateways registered.

SMG Operation

- S1 of sets is configured to Node IP of SMG
  - Always register to redundant node first
  - Sets are redirected by NCS on NRS to Main Office
- Sets in NORMAL MODE display
  - USER: XYYYEXTN e.g.USER:91211000
    - X-AC code YYY-Location Code EXTN-Extension
- Test LOCAL MODE
  - SERVICES key on phone
    - Test Local Mode
    - Resume Normal Mode
- Disable ELAN on Main Office to Test operation in Survivable mode.
  - LD 137 - DIS ELNK
  - On SMG – LD 135 - STAT GR
    - Observe License change from Inactive to Activating to Active
    - Also lists Sets & Media Gateways registered

378

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

30. PCAP – Packet Capture

PCAP or Packet Capture is used to analyse the information passing on your network between different devices. Basically it sets the Ethernet controller in to a mode where it collects every packet it sees on the Network, whether addressed to the system you are on or not.

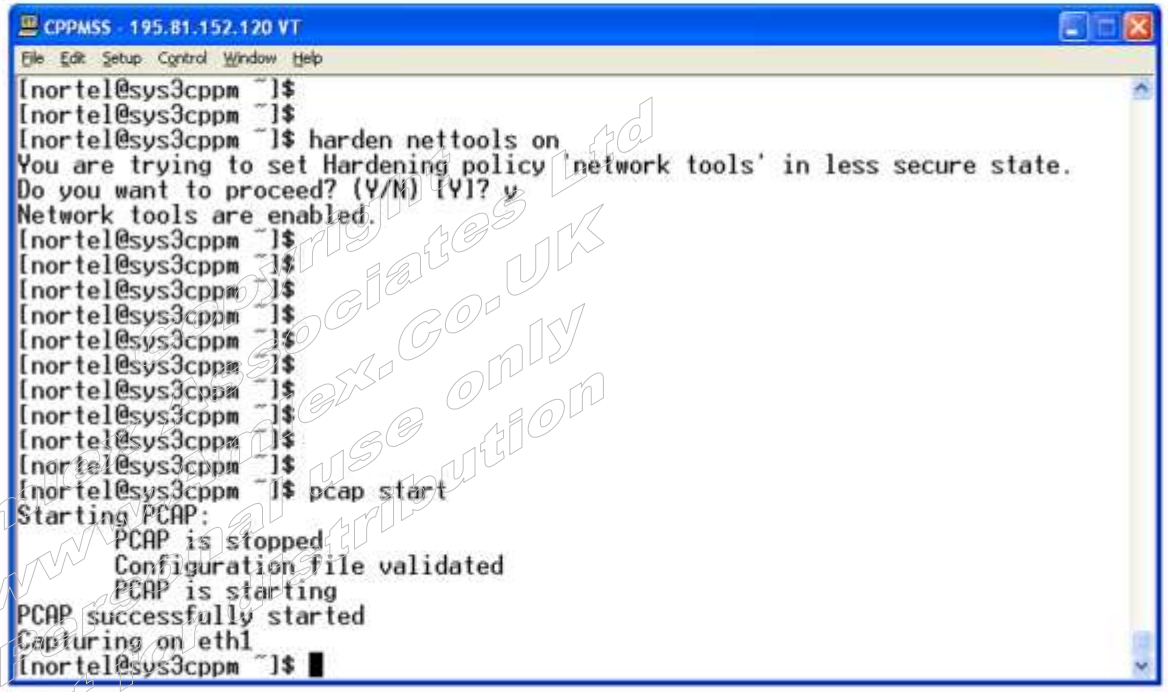
Normally you would need to set up a Mirror Port on an Ethernet Switch to collect this data which is complex and time consuming. However the Linux Base software has PCAP built-in thus allowing capture to be done directly on the server.

Firstly however you need to enable PCAP by using the command

$harden nettools on

This allows PCAP to be used, it is then a case of starting PCAP as shown

$pcap start Start Capture
$pcap stop Stop Capture


CPPMSS - 195.81.152.120 VT
File Edit Setup Control Window Help
[nortel@sys3cppm ~]$
[nortel@sys3cppm ~]$
[nortel@sys3cppm ~]$ harden nettools on
You are trying to set Hardening policy 'network tools' in less secure state.
Do you want to proceed? (Y/N) [Y]? y
Network tools are enabled.
[nortel@sys3cppm ~]$ pcap start
Starting PCAP:
PCAP is stopped
Configuration file validated
PCAP is starting
PCAP successfully started
Capturing on eth1
[nortel@sys3cppm ~]$

379

Notes

_____
_____
_____
_____

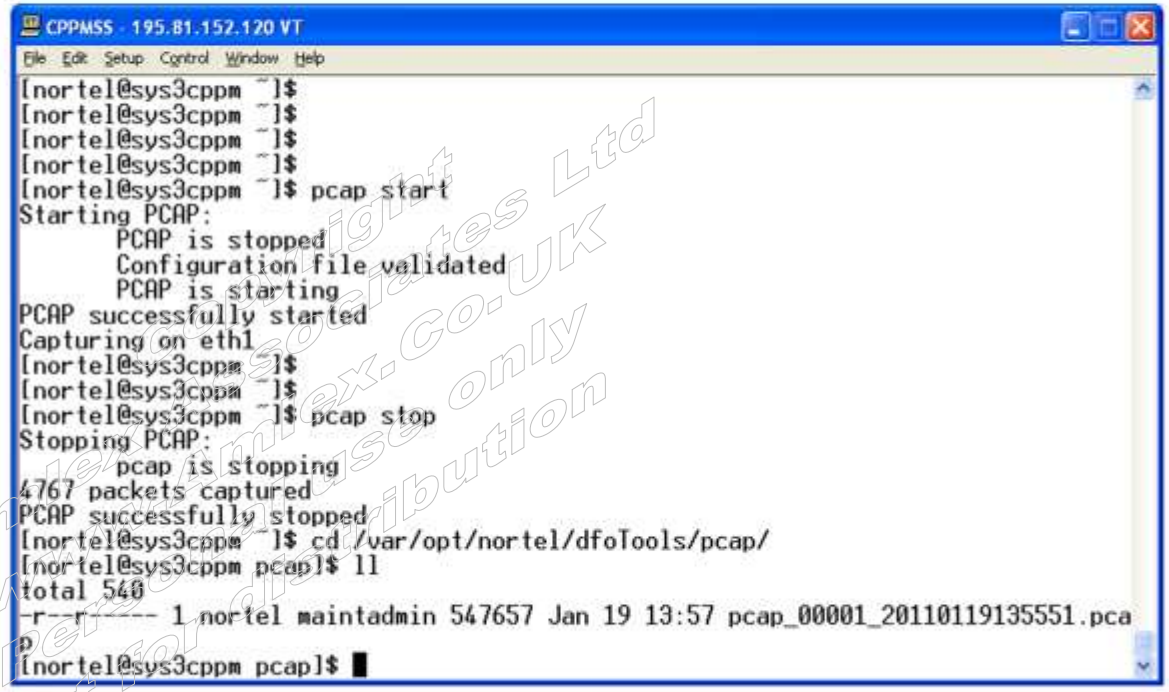
Copyright Amlex Associates Ltd

Start & Stop PCAP

The file created is stored in the directory

/var/opt/nortel/dfoTools/pcap

The easiest way to move it from the Linux server to your PC for analysis is to use an SFTP client such as FileZilla.



Amlex Copyright
www.amlex.co.uk
Personal use only
Not for distribution

380

Notes

_____

_____

_____

_____

Wireshark

Once you have the file on your PC you can open it with Wireshark to inspect the packets.

Remember that some packets are proprietary to Nortel (RUDP) and you will not be able to read the contents.

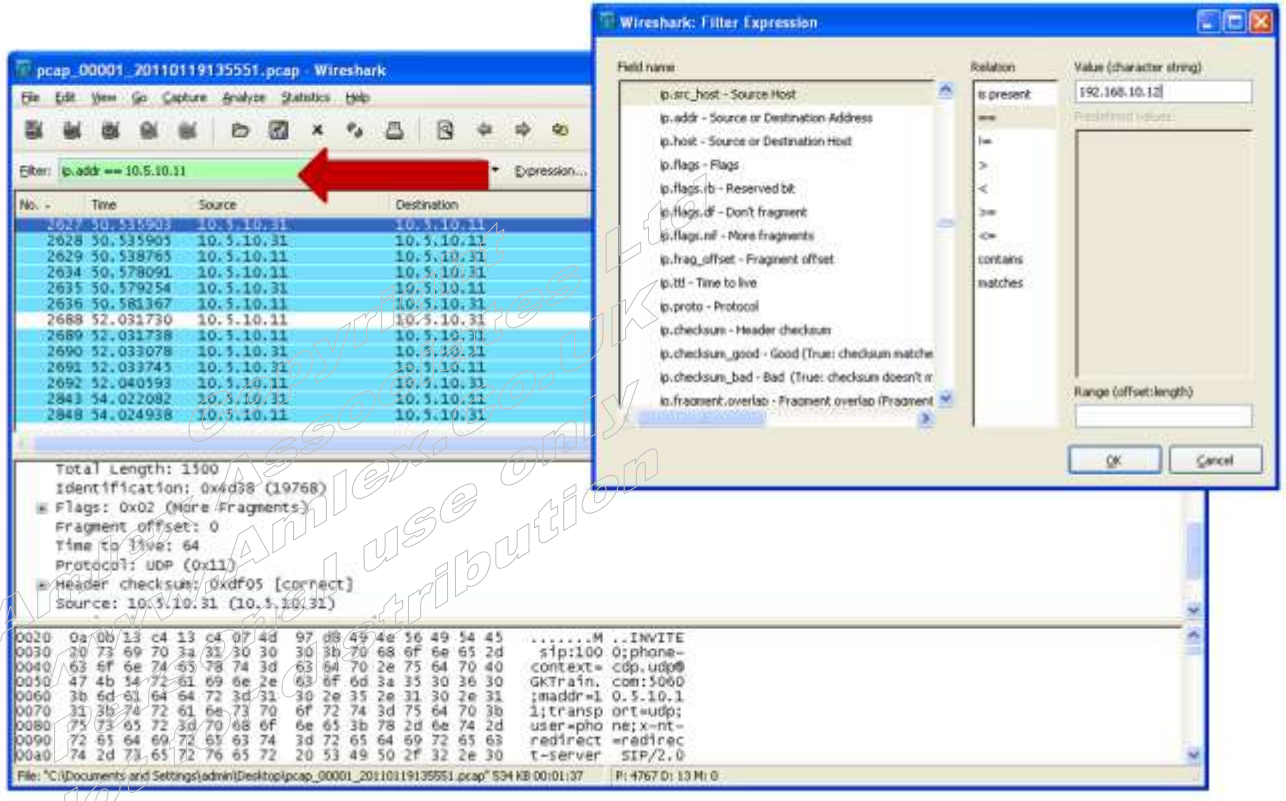
Note the use of EXPRESSION to filter the packets used.

Wireshark can also be used to collect data directly for you PC's Ethernet device using the Capture Menu.

Using this method and an IP Phone you can even collect and replay a conversation.

Connect the PC to the PC port of the IP phone you are using and then set the PC port into Mirror mode by issuing the sequence

Mute, Up Arrow, Down Arrow, Up Arrow, Down Arrow, Up Arrow, mute, 7, release


pcap_00001_20110119135551.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr == 10.5.10.11
Expression...
No. - Time Source Destination
2627 50.535903 10.5.10.31 10.5.10.11
2628 50.535905 10.5.10.31 10.5.10.11
2629 50.538765 10.5.10.11 10.5.10.31
2634 50.578091 10.5.10.11 10.5.10.31
2635 50.579254 10.5.10.31 10.5.10.11
2636 50.581367 10.5.10.11 10.5.10.31
2688 52.031730 10.5.10.11 10.5.10.31
2689 52.031738 10.5.10.31 10.5.10.11
2690 52.033078 10.5.10.31 10.5.10.11
2691 52.033745 10.5.10.31 10.5.10.11
2692 52.040593 10.5.10.11 10.5.10.31
2843 54.022082 10.5.10.31 10.5.10.11
2848 54.024938 10.5.10.11 10.5.10.31
Total Length: 1500
Identification: 0x4d38 (19768)
Flags: 0x02 (More Fragments)
Fragment offset: 0
Time to live: 64
Protocol: UDP (0x11)
Header checksum: 0xdf05 [correct]
Source: 10.5.10.31 (10.5.10.31)
0020 0a 0b 13 c4 13 c4 07 4d 97 d8 49 4e 56 49 54 45 ....M ..INVITE
0030 20 73 69 70 3a 31 30 30 30 3b 70 68 6f 6e 65 2d sip:100 0;phone-
0040 63 6f 6e 74 65 78 74 3d 63 64 70 2e 75 64 70 40 context= cdp.udp@
0050 47 4b 54 72 61 69 6e 2e 63 6f 6d 3a 35 30 36 30 GKTrain. com:5060
0060 3b 6d 61 64 64 72 3d 31 30 2e 35 2e 31 30 2e 31 ;maddr=1 0.5.10.1
0070 31 3b 74 72 61 6e 73 70 6f 72 74 3d 75 64 70 3b 1;transp ort=udp;
0080 75 73 65 72 3d 70 68 6f 6e 65 3b 78 2d 6e 74 2d user=pho ne;x-nt-
0090 72 65 64 69 72 65 63 74 3d 72 65 64 69 72 65 63 redirect =redirec
00a0 74 2d 73 65 72 76 65 72 20 53 49 50 2f 32 2e 30 t-server SIP/2.0
File: "C:\Documents and Settings\admin\Desktop\pcap_00001_20110119135551.pcap" 534 KB 00:01:37
P: 4767 D: 13 M: 0
Wireshark: Filter Expression
Field name
Relation
Value (character string)
ip.src_host - Source Host
ip.addr - Source or Destination Address
ip.host - Source or Destination Host
ip.flags - Flags
ip.flags.rb - Reserved bit
ip.flags.df - Don't fragment
ip.flags.mf - More fragments
ip.frag_offset - Fragment offset
ip.ttl - Time to live
ip.proto - Protocol
ip.checksum - Header checksum
ip.checksum_good - Good (True: checksum matche
ip.checksum_bad - Bad (True: checksum doesn't m
ip.fragment.overlap - Fragment overlap (Fragment
is present
==
!=
>
<
>=
<=
contains
matches
192.168.10.12
Range (offset:length)
OK
Cancel

381

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd
Not for Amlex use only
No distribution

Select Records & Decode

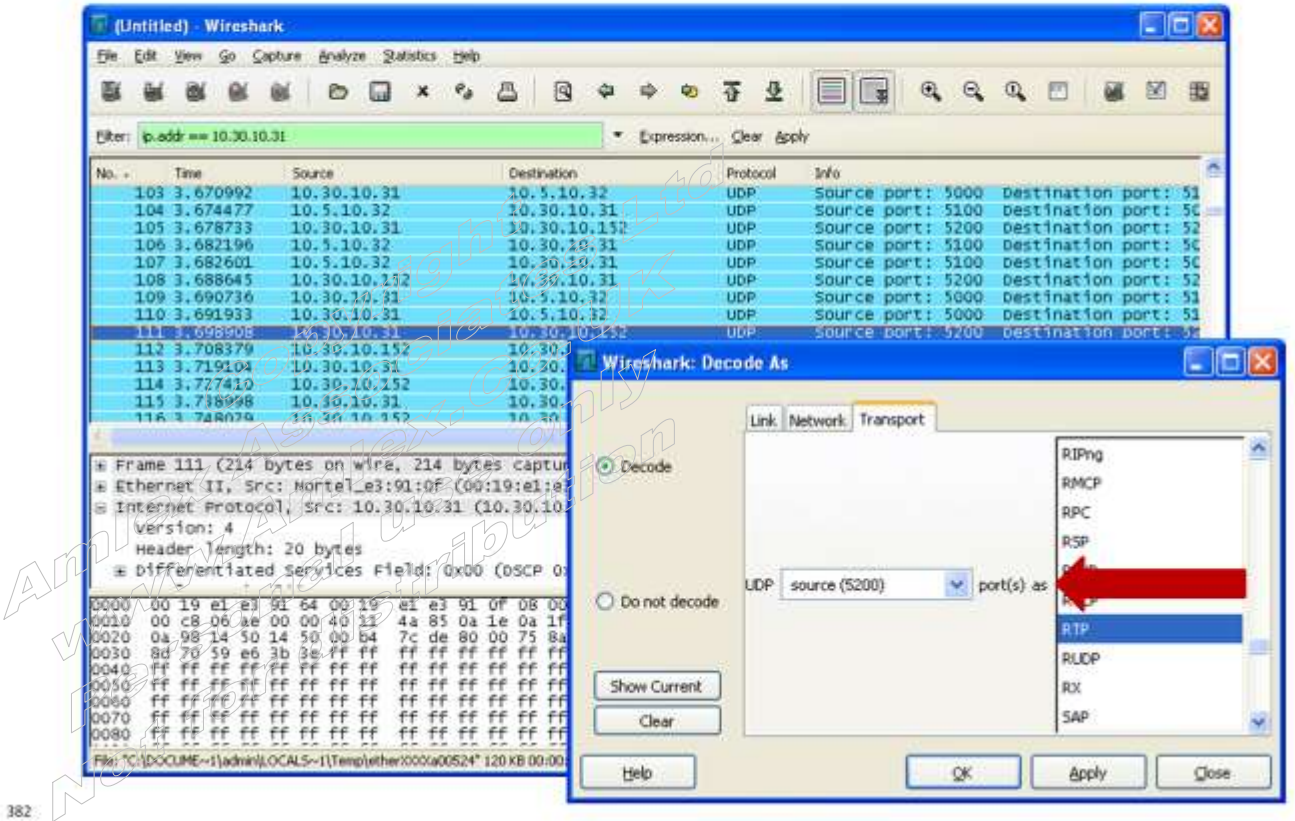
Once you have collected some records and filtered the ones you want to look at, find a UDP record using Port 5200 as shown and select it.

Using the menu option

ANALYZE / DECODE AS

Select the option to decode as RTP (Real Time Protocol). This will show the RTP information for all packets in the stream.

See next slide.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr == 10.30.10.31
Expression... Clear Apply
No. Time Source Destination Protocol Info
103 3.670992 10.30.10.31 10.5.10.32 UDP Source port: 5000 Destination port: 51
104 3.674477 10.5.10.32 10.30.10.31 UDP Source port: 5100 Destination port: 5C
105 3.678733 10.30.10.31 10.30.10.152 UDP Source port: 5200 Destination port: 52
106 3.682196 10.5.10.32 10.30.10.31 UDP Source port: 5100 Destination port: 5C
107 3.682601 10.5.10.32 10.30.10.31 UDP Source port: 5100 Destination port: 5C
108 3.688645 10.30.10.152 10.30.10.31 UDP Source port: 5200 Destination port: 52
109 3.690736 10.30.10.31 10.5.10.32 UDP Source port: 5000 Destination port: 51
110 3.691933 10.30.10.31 10.5.10.32 UDP Source port: 5000 Destination port: 51
111 3.698908 10.30.10.31 10.30.10.152 UDP Source port: 5200 Destination port: 52
112 3.708379 10.30.10.152 10.30.
113 3.719104 10.30.10.31 10.30.
114 3.727410 10.30.10.152 10.30.
115 3.738998 10.30.10.31 10.30.
116 3.748079 10.30.10.152 10.30.
Frame 111 (214 bytes on wire, 214 bytes captu
Ethernet II, Src: Nortel_e3:91:0f (00:19:e1:e
Internet Protocol, Src: 10.30.10.31 (10.30.10.
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0
0000 00 19 e1 e3 91 64 00 19 e1 e3 91 0f 08 00
0010 00 c8 06 ae 00 00 40 11 4a 85 0a 1e 0a 1f
0020 0a 98 14 50 14 50 00 b4 7c de 80 00 75 8a
0030 8d 70 59 e6 3b 3e ff ff ff ff ff ff ff ff
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff
File: "C:\DOCUME~1\admin\LOCALS~1\Temp\ether0000a00524" 120 KB 00:00:
Wireshark: Decode As
Link Network Transport
Decode
Do not decode
UDP source (5200) port(s) as
RIPng
RMCP
RPC
RSP
RTP
RUDP
RX
SAP
Show Current
Clear
Help
OK
Apply
Close

382

Notes

_____

_____

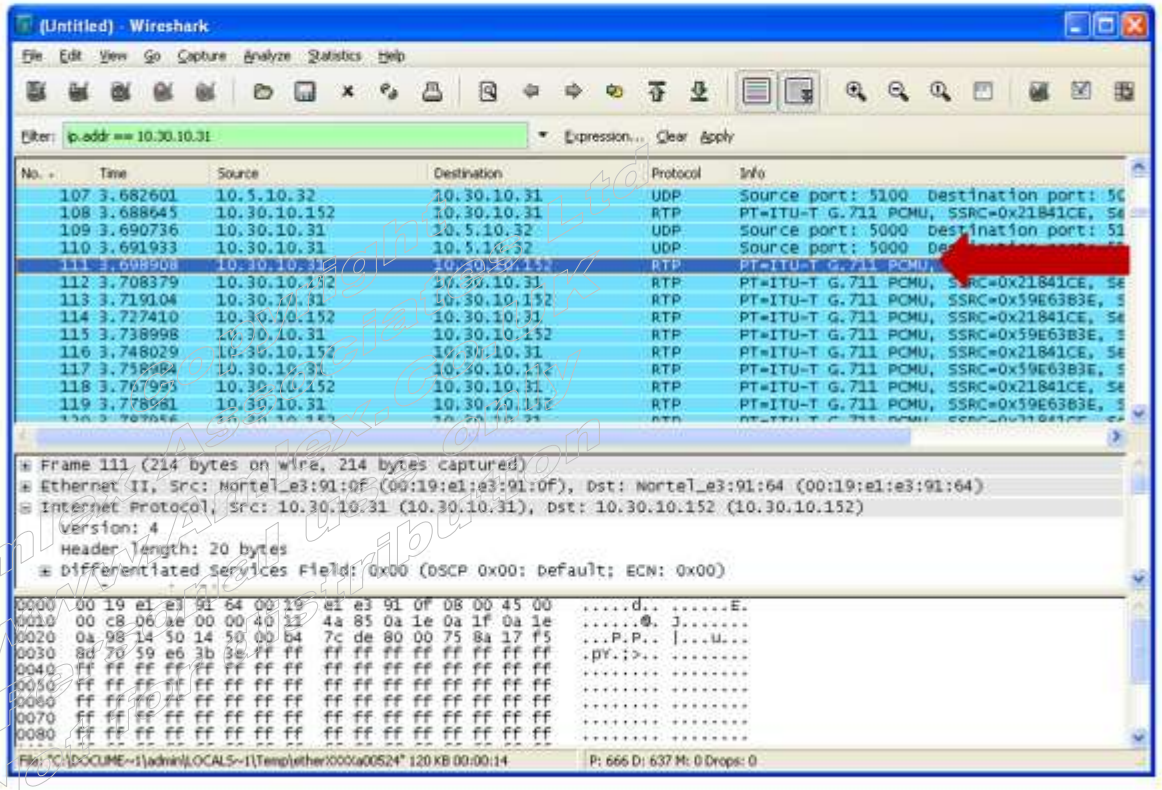
_____

_____

Copyright Amlex Associates Ltd

Decoded to RTP

Here you can see the decoded packets showing the Codec used to create them, as well as more RTP information such as SSRC etc.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: ip.addr == 10.30.10.31
Expression... Clear Apply
No. Time Source Destination Protocol Info
107 3.682601 10.5.10.32 10.30.10.31 UDP Source port: 5100 Destination port: 5C
108 3.688645 10.30.10.152 10.30.10.31 RTP PT=ITU-T G.711 PCMU, SSRC=0x21841CE, Se
109 3.690736 10.30.10.31 10.5.10.32 UDP Source port: 5000 Destination port: 51
110 3.691933 10.30.10.31 10.5.10.32 UDP Source port: 5000 De
111 3.698508 10.30.10.31 10.30.10.152 RTP PT=ITU-T G.711 PCMU,
112 3.708379 10.30.10.152 10.30.10.31 RTP PT=ITU-T G.711 PCMU, SSRC=0x21841CE, Se
113 3.719104 10.30.10.31 10.30.10.152 RTP PT=ITU-T G.711 PCMU, SSRC=0x59E63B3E, S
114 3.727410 10.30.10.152 10.30.10.31 RTP PT=ITU-T G.711 PCMU, SSRC=0x21841CE, Se
115 3.738998 10.30.10.31 10.30.10.152 RTP PT=ITU-T G.711 PCMU, SSRC=0x59E63B3E, S
116 3.748029 10.30.10.152 10.30.10.31 RTP PT=ITU-T G.711 PCMU, SSRC=0x21841CE, Se
117 3.758984 10.30.10.31 10.30.10.152 RTP PT=ITU-T G.711 PCMU, SSRC=0x59E63B3E, S
118 3.767993 10.30.10.152 10.30.10.31 RTP PT=ITU-T G.711 PCMU, SSRC=0x21841CE, Se
119 3.778981 10.30.10.31 10.30.10.152 RTP PT=ITU-T G.711 PCMU, SSRC=0x59E63B3E, S
Frame 111 (214 bytes on wire, 214 bytes captured)
Ethernet II, Src: Nortel_e3:91:0f (00:19:e1:e3:91:0f), Dst: Nortel_e3:91:64 (00:19:e1:e3:91:64)
Internet Protocol, Src: 10.30.10.31 (10.30.10.31), Dst: 10.30.10.152 (10.30.10.152)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
0000 00 19 e1 e3 91 64 00 19 e1 e3 91 0f 08 00 45 00 .....d.. ......E.
0010 00 c8 06 ae 00 00 40 11 4a 85 0a 1e 0a 1f 0a 1e ......@. J.......
0020 0a 98 14 50 14 50 00 b4 7c de 80 00 75 8a 17 f5 ...P.P.. |...u...
0030 8d 70 59 e6 3b 3e ff ff ff ff ff ff ff ff ff ff .pY.;>.. ....
0040 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0050 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0060 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0070 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
0080 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ....
File: "C:\DOCUME~1\admin\LOCALS~1\Temp\ether0000a00524" 120 KB 00:00:14
P: 666 D: 637 M: 0 Drops: 0

383

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

STATISTICS /RTP/SHOW ALL STREAMS

If you now use the Menu Option :-

STATISTICS/RTP/SHOWALL STREAMS

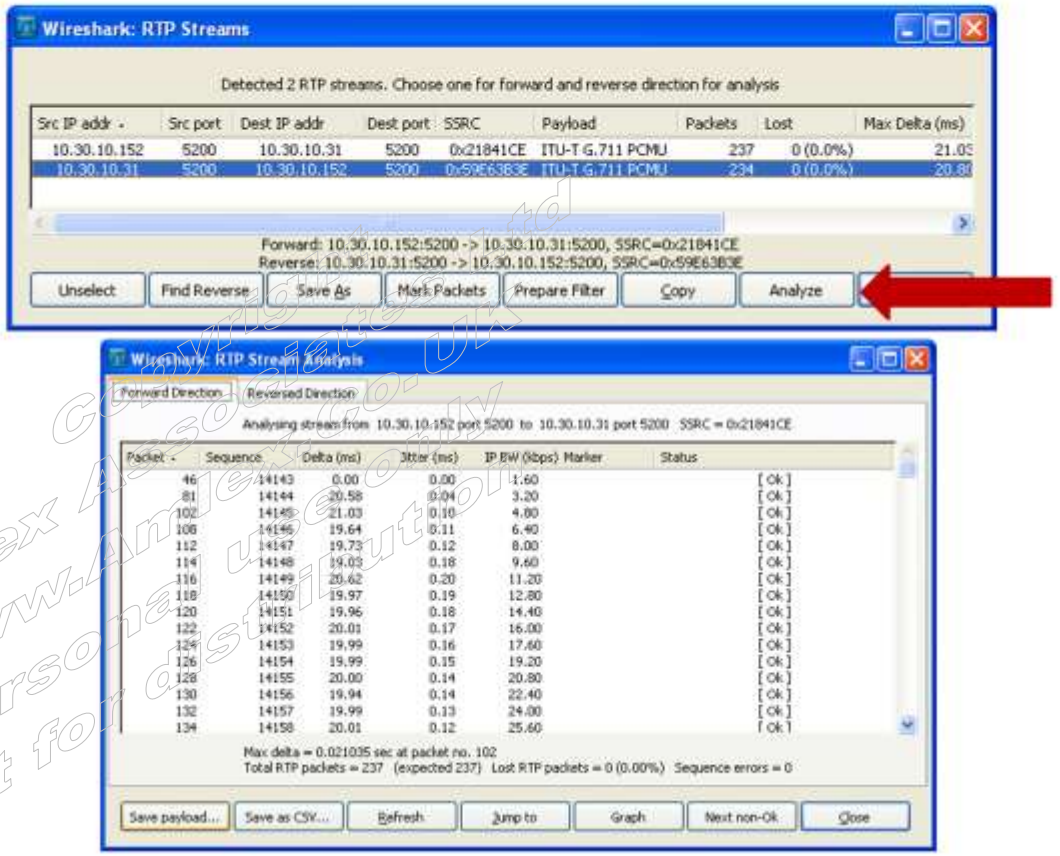
You will be presented with the dialogue shown here (top) . To Analyse the streams you need to select the Forward and Reverse streams (Select one then shift to select the second) make sure both are selected as Forward and Reverse as shown here.

Then clicking on the **ANALYZE** button will show the RTP data including things like the Jitter on each packet.

To save this as an audio file select the

SAVE PAYLOAD

Button as shown


Wireshark: RTP Streams
Detected 2 RTP streams. Choose one for forward and reverse direction for analysis
Src IP addr | Src port | Dest IP addr | Dest port | SSRC | Payload | Packets | Lost | Max Delta (ms)
10.30.10.152 | 5200 | 10.30.10.31 | 5200 | 0x21841CE | ITU-T G.711 PCMU | 237 | 0 (0.0%)
10.30.10.31 | 5200 | 10.30.10.152 | 5200 | 0x59E63B3E | ITU-T G.711 PCMU | 234 | 0 (0.0%)
Forward: 10.30.10.152:5200 -> 10.30.10.31:5200, SSRC=0x21841CE
Reverse: 10.30.10.31:5200 -> 10.30.10.152:5200, SSRC=0x59E63B3E
Unselect
Find Reverse
Save As
Mark Packets
Prepare Filter
Copy
Analyze
Wireshark: RTP Stream Analysis
Forward Direction
Reversed Direction
Analysing stream from 10.30.10.152 port 5200 to 10.30.10.31 port 5200 SSRC = 0x21841CE
Packet | Sequence | Delta (ms) | Jitter (ms) | IP BW (kbps) | Marker | Status
Max delta = 0.021035 sec at packet no. 102
Total RTP packets = 237 (expected 237) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Save payload...
Save as CSV...
Refresh
Jump to
Graph
Next non-Ok
Close

384

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

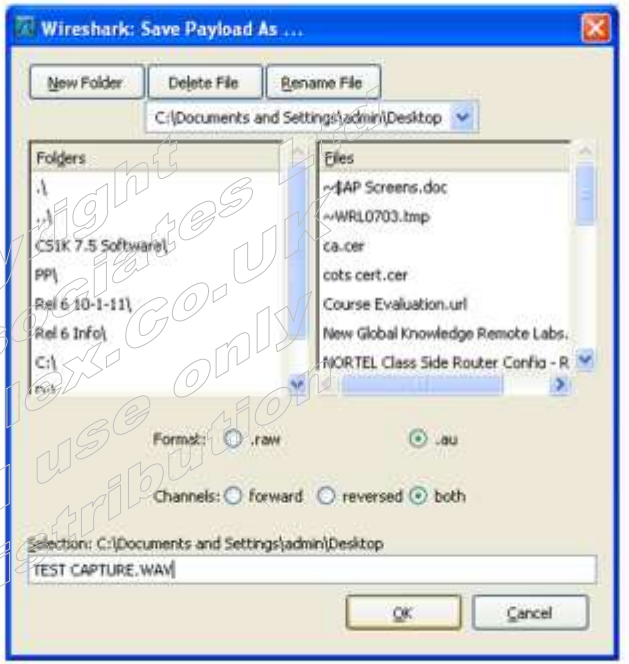
SAVE PAYLOAD

When saving the file make sure you select the Format .au and select both streams. Also when saving add the extension .WAV to ensure it can be easily played on your PC.

NOTE:-

Only calls using G.711 can be captured and decoded in this manner.

To decode G729 calls an offline application is used after saving the packet stream.



Copyright Amlex Associates Ltd
www.Amlex.Co.Uk
Personal use only
Not for distribution

385

Notes

_____

_____

_____

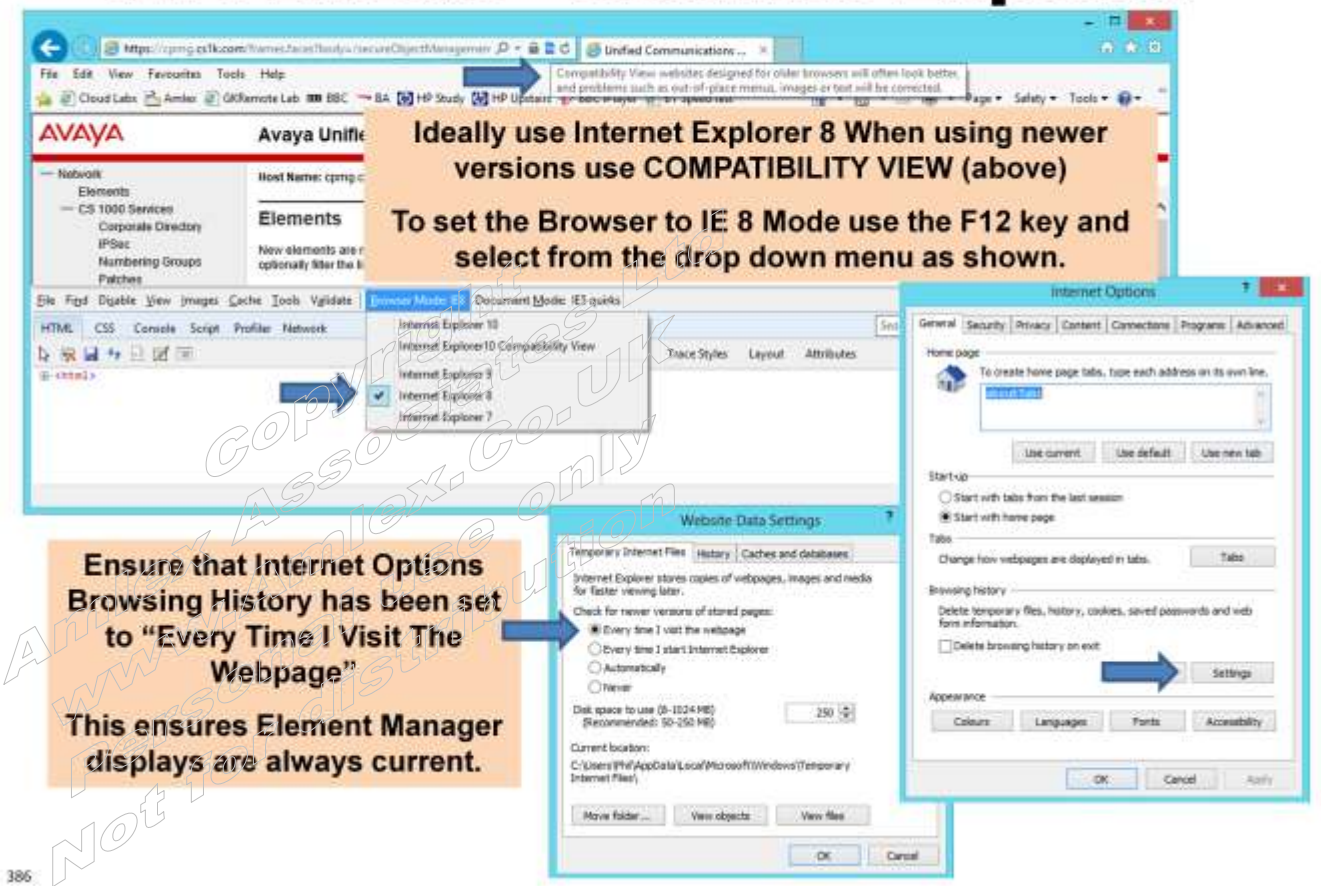
_____

APPENDIX – Internet Explorer

Internet Explorer is the only web browser supported by the CS1000 system. However the only version which will give minimal issues is IE 8.

Firstly no matter which version of browser you use, you need to set the Browsing History to "Every Time I Visit The Webpage" as shown at the bottom of the display. This ensures that the correct information is displayed in Element Manager, rather than cached information which could be out of date.

When using newer versions of Internet Explorer (later than Rel 8) many displays will be shown distorted or fail to display at all. Most of these instances can be corrected by setting the Compatibility mode as shown at the top of the display. In addition the browser can be set into IE 8 Mode using the F12 key (this accesses debug options) and then selecting BROWSER MODE IE8 from the drop down menu. This will correct many of the problems but you may still suffer some issues.


Ideally use Internet Explorer 8 When using newer versions use COMPATIBILITY VIEW (above)
To set the Browser to IE 8 Mode use the F12 key and select from the drop down menu as shown.
Ensure that Internet Options Browsing History has been set to "Every Time I Visit The Webpage"
This ensures Element Manager displays are always current.
Internet Options
Website Data Settings
386

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Setting A law & UK Tones

Note some prompts have been omitted in the listing shown.

Need to reboot for tones and law changes to take affect.

Note when building PRI trunks set PCML to A to match switch law else crackling voice quality.

```
LD 17
REQ chg
Type atrn
Code 2 (0)
```

```
LD 17
REQ chg
Type parm
Pcml a (mu)
```

```
LD 97
Req Chg
Type xctp
Dtmf 138 (14)
```

```
LD 97
Req Chg
Type sysp
Intn yes
```

LD 56 Changing essential tones & cadences

```
Req New
Type fcad
Wcad 32
Cndc 80 40 80 400
End rept
Cycs 1 2

REQ  chg                    LD 56
TYPE ftc
TABL 0
RING
HCCT yes
DIAL
XTON        129
Xcad        0
Busy
XTON        130
Xcad        30
RGBK
XTON        132
Xcad        32
OVFL
XTON        130
Xcad        0
```

Copyright Amlex Associates Ltd www.Amlex.Co.UK Personal use only Not for distribution

387

Notes

_____

_____

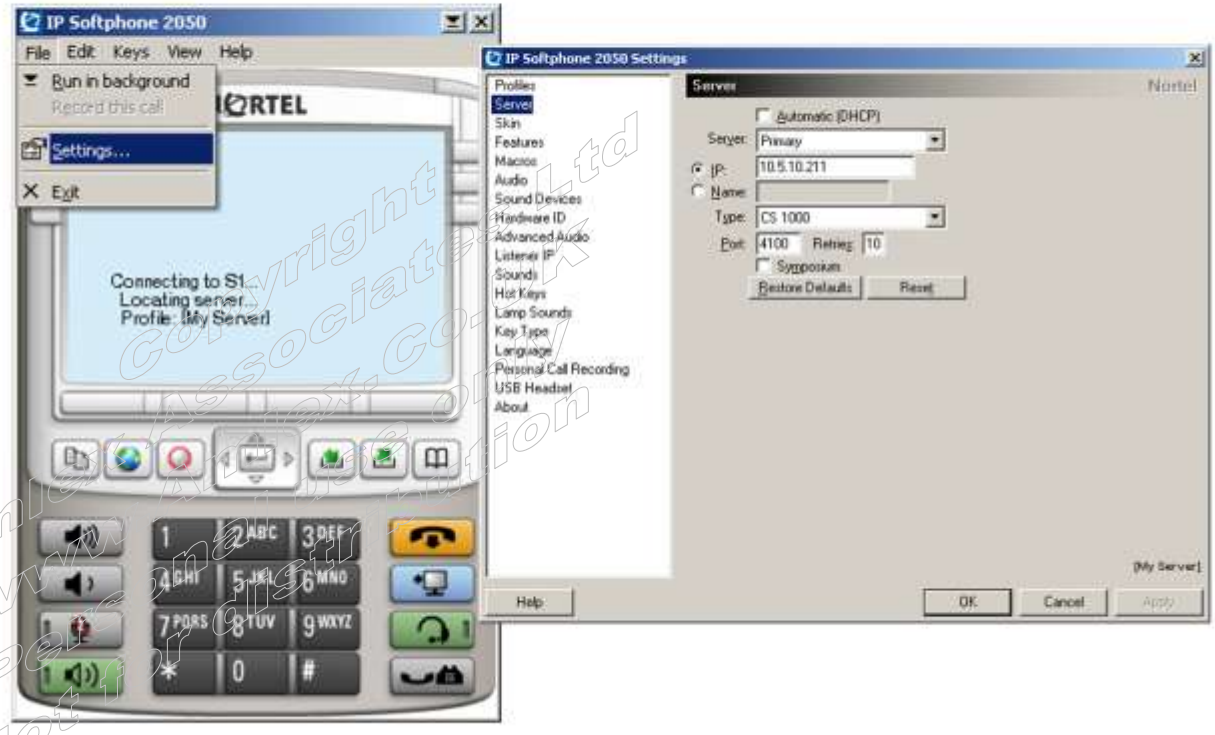
_____

_____

Configuring SoftPhone

Select the Settings option from the FILE Menu and set the S1 Address by disabling the DHCP Option and selecting the IP Radio button.

You may also need to select the correct SOUND DEVICE and USB HEADSET to correctly receive the audio.



388

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

PAD Table Settings

- Pad Table Settings
  - Required for Media Cards
  - Sets levels for the card

CS 1000S DTI/PRI Prompt	Norway		Sweden		Switzerland		UK	
	Rx Code	Tx Code	Rx Code	Tx Code	Rx Code	Tx Code	Rx Code	Tx Code
ONP	5	6	14	3	3	3	6	5
DSET	4	7	7	7	7	4	3	4
OPX*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DTT	0	0	0	0	0	0	0	0
SDTT	0	0	0	0	0	0	0	0
DCO*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DTO	3	19	3	19	3	19	3	19
VNL	0	0	0	0	0	0	0	0
SATT	3	19	3	19	3	19	3	19
ACO	0	16	18	18	17	15	2	16
ATO	3	19	3	19	3	19	3	19
PRI	0	0	0	0	0	0	0	0
PRI2	0	0	0	0	0	0	0	0
XUT	15	2	19	0	18	3	1	2
XEM	16	16	19	1	19	1	2	16
BRIL	0	0	0	0	0	0	0	0
BRIT	0	0	0	0	0	0	0	0
WRLS	3	19	3	19	3	19	3	19

Note: * OPX and DCO do not apply for these countries. Press <cr> for these prompts.

Note: The DASS/DPNSS interface to MG 1000S loss is adjusted by changing the PRI2 entry.

389

Copyright Amlex Associates Ltd
www.Amlex.Co.UK
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

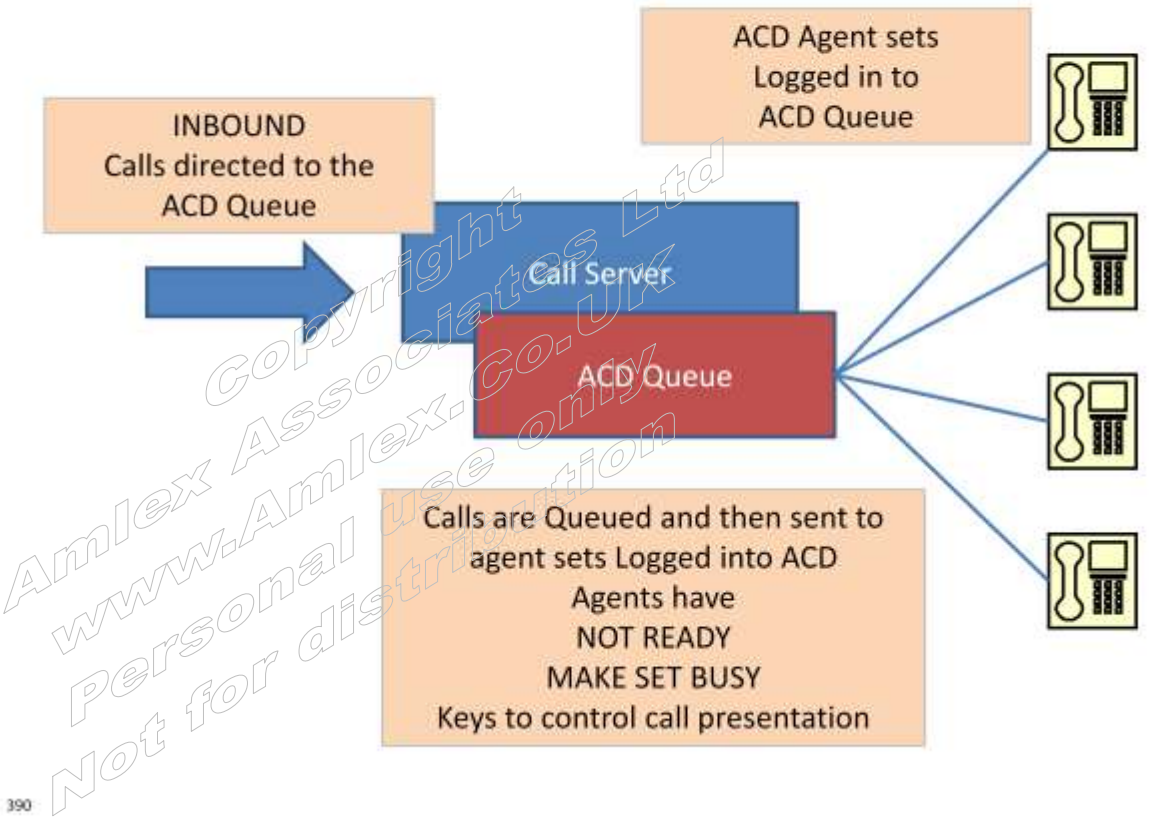
Automatic Call Distribution

Automatic Call Distribution (ACD) is the simple way to queue calls to a number of users in an ACD group.

The ACD has its own number which callers are directed to on the Call Server. The ACD itself has Agent Positions allocated to it by the set programming. When these are available to take calls i.e. Logged in and Ready, calls will be offered from the queue to the agent positions.

In this way calls can be queued and receive announcements or continuous ringing rather than a busy tone.

Further control can be added by using a Control DN (CDN). This is becomes the published DN but allows further flexibility e.g. “Ceiling” to control the total number of calls queued . The CDN ultimately passes the call to the ACD DN for processing.



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

_____

Create ACD Queue in Overlays

The ACD itself is created in Overlay 23.

The example here is a simple ACD queue which has the DN 2500 and a Maximum number of positions of 10.

Note as with many system options the ACD is allocated to a specific Customer.

LD 23

NEW	
TYPE ACD	Automatic Call Distribution
CUST 0	Customer Number Usually 0
ACDN 2500	ACD DN number to be used
MWC NO	
DSAC NO	
MAXP 10	Maximum No. Positions
SDNB NO	
BSCW NO	
ISAP NO	
AACQ NO	
RGAI NO	
ACAA NO	
----------	Use defaults for the rest of the prompts

Amlex Associates Ltd Copyright
www.Amlex.Co.Uk
Personal use only
Not for distribution

391

Notes

_____

_____

_____

_____

Create ACD Sets

Finally we need to create some ACD sets to utilise the queue. This can be done in either the Overlays (11 or 20) or via the Element Manager as shown here.

Note that the ACD is always assigned to KEY 0.

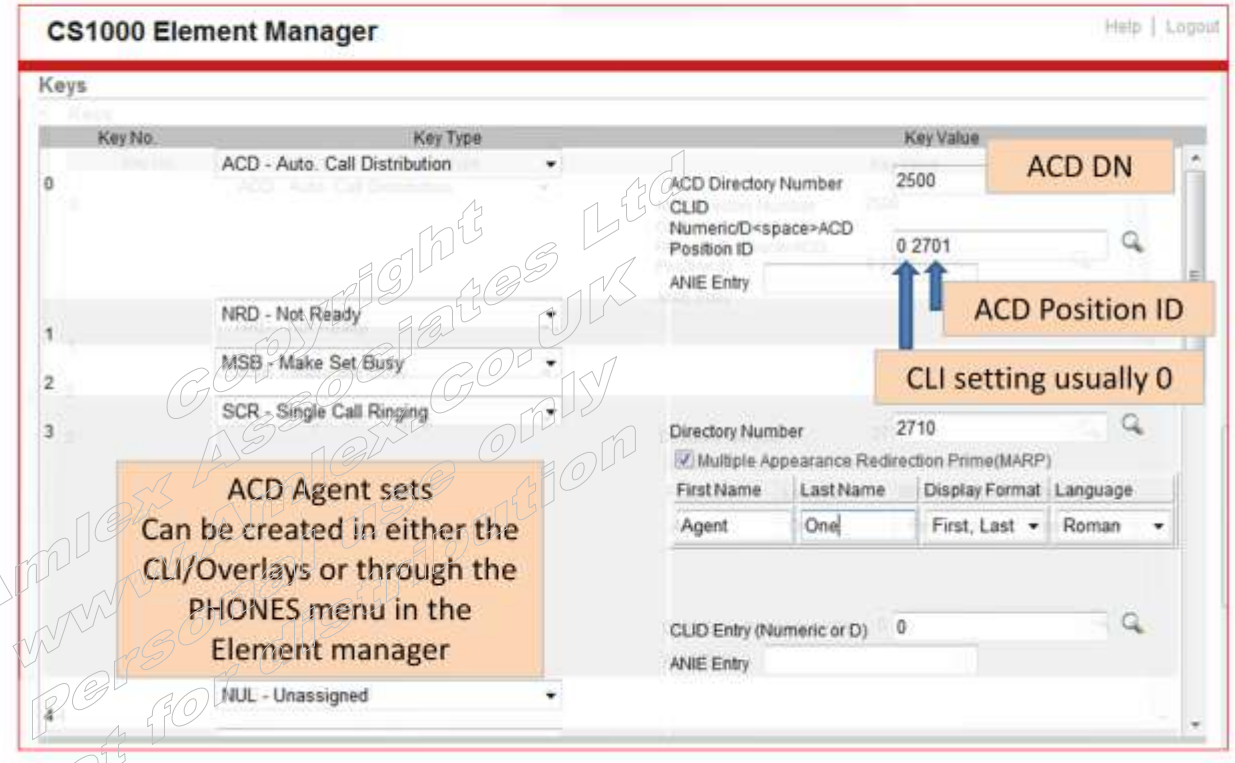
Here you can see the ACD DN and the CLI/Position Number assigned to it.

In the Overlays this would be done as :-
>KEY 0 ACD xxxx 0 yyyy

Where :-

xxxx	**ACD DN**
0	**CLI (Usually 0)**
yyyy	**ACD Position ID**

Note also the NRD & MSB keys which will control the agent phones ability to take calls. Finally Key 3 has been allocated its own DN so the agent can make calls outside of the ACD.



Copyright Amlex Associates Ltd
Amlex Associates Ltd
www.amlex.co.uk
Personal use only
Not for online distribution

392

Notes

_____

_____

_____

_____

There is also an option to type <CTRL>B when the card boots to halt it at the VxWorks boot prompt.

From here you can access the “test” menu (type test) which allow you to change the Boot options for the card. Setting CSP & MSP to Gold image will allow you to halt the card using the <CTRL>i option after VxWorks has started . Then you can issue the mgcIPClear and diskformat commands if required to set the card back to day one defaults.

The <CTRL>i option is only available when booted from the Gold Image. Once the card has downloaded the update Loadware this option will not be displayed and you will need to use either <CTRL>oam or <CTRL>ldb to login to the card.

NOTE:- MGC/MGS cards can be accessed across the network using SSH (e.g. Putty).

MGC/MGS Commands

MGC – Clearing & Resetting

The Media Gateway Controller once configured will not respond to a c/r.

To login there are two modes ldb & oam, Local Database Mode or Operations and Maintenance

These are accessed by typing <ctrl> ldb or <ctrl> oam

To login to ldb mode you will need a pdt2 level password or Network Administrator role

Useful MGC commands

mgcsetup – runs the configuration programme to setup the IP addresses for the card. If the card is cleared or new this runs automatically.

mgcIPClear – Clears the IP addresses from the non-volatile RAM on the card.

diskformat – Formats the Compact Flash on the MGC card. This removes any software from it downloaded from the Call Server.

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

393

Notes

_____

_____

_____

_____

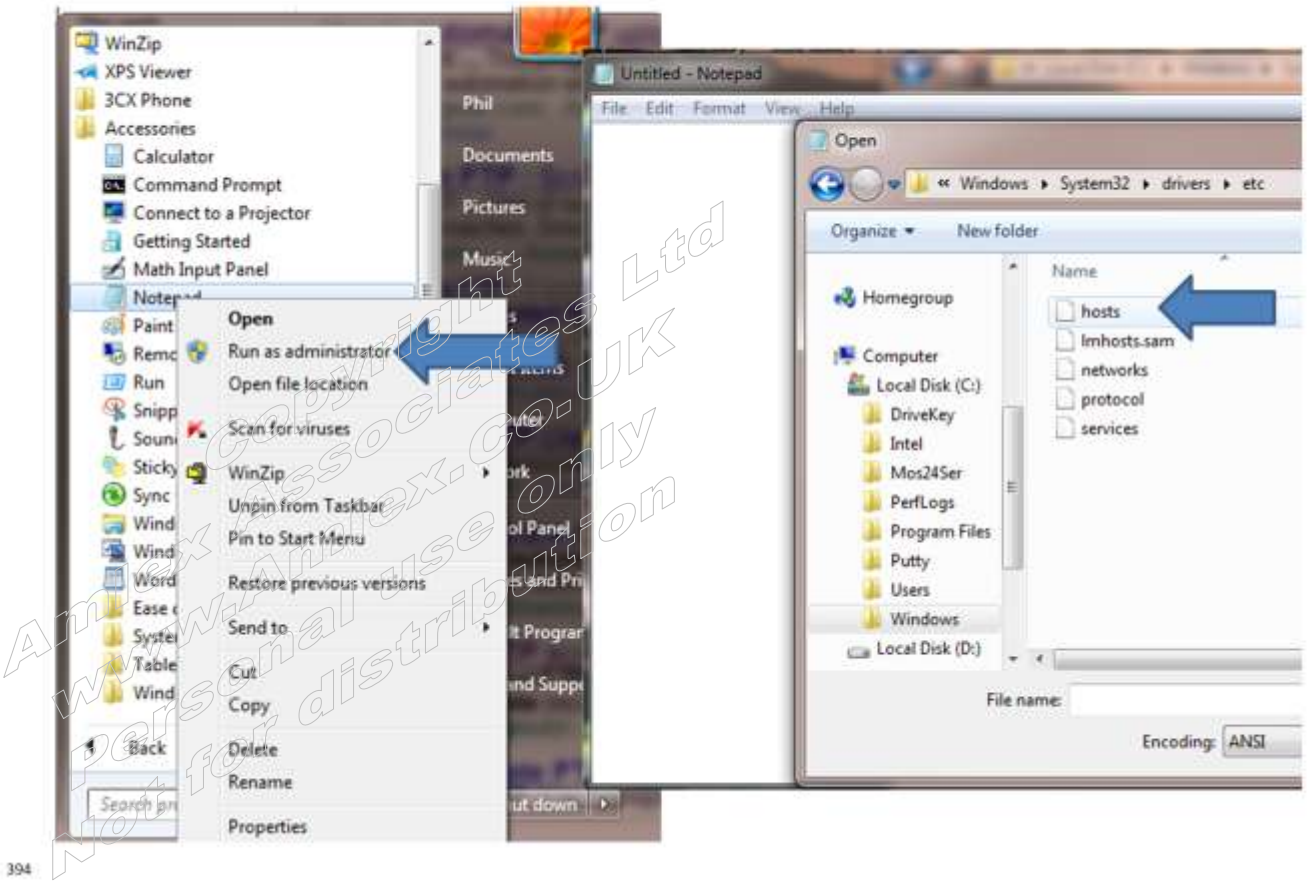
Edit PC Hosts File

If you are not using a DNS on the network then you will need to add an entry to the HOSTS file on the PC managing the switch to enable the use of the FQDN.

The file is located in the directory :-

C:\Windows\System32\drivers\etc

To edit the file use Notepad. Be aware that if you are running Windows 7 or Vista you need to run Notepad as Administrator as shown to enable saving the file correctly



Copyright Amlex Associates Ltd www.Amlex.co.UK Personal use only Not for distribution

Notes

_____

_____

_____

_____

Add Host to File

To enable the FQDN resolution to an IP address add a line at the bottom of the file similar to that shown in the example.

TLAN IP Address Server FQDN

Save the file and test the resolution by trying a ping from a DOS window to the FQDN. e.g.

>ping CPPM-Cores.CS1K.com

The result should return the IP address of the server.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.0.130           CPPM-CoRes.CS1K.Amlex.Co.UK
```

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

395

Notes

_____

_____

_____

_____

IMPORTANT NOTE FOR USERS OF VISTA & WIN 7

Please note that if you are running Windows Vista or Windows 7 the enhanced security of these operating systems will prevent the correct formatting of the Compact Flash card.

In order to overcome this you need to locate the syslinux file inside the utilities folder and edit the properties so that it always runs with the administrator privilege.

Be aware you will get a Windows message asking you to proceed when you are formatting the CF .

Create Linux Installer CF or USB

- Locate Software
  - Expand if necessary
- From Utilities Folder
  - Change syslinux to run as administrator on Vista & Win 7
  - Run mkbootrmd
    - Enter USB or CF Drive letter
    - Select whether USB or CF to be created
    - Ensure Format & installation of BOOT Sector are successful
- Copy Software files to CF
- Add keycode folder
  - Copy keycodes to folder

Copyright Amlex Associates Ltd www.amlex.co.uk Personal use only Not for distribution

396

Notes

_____

_____

_____

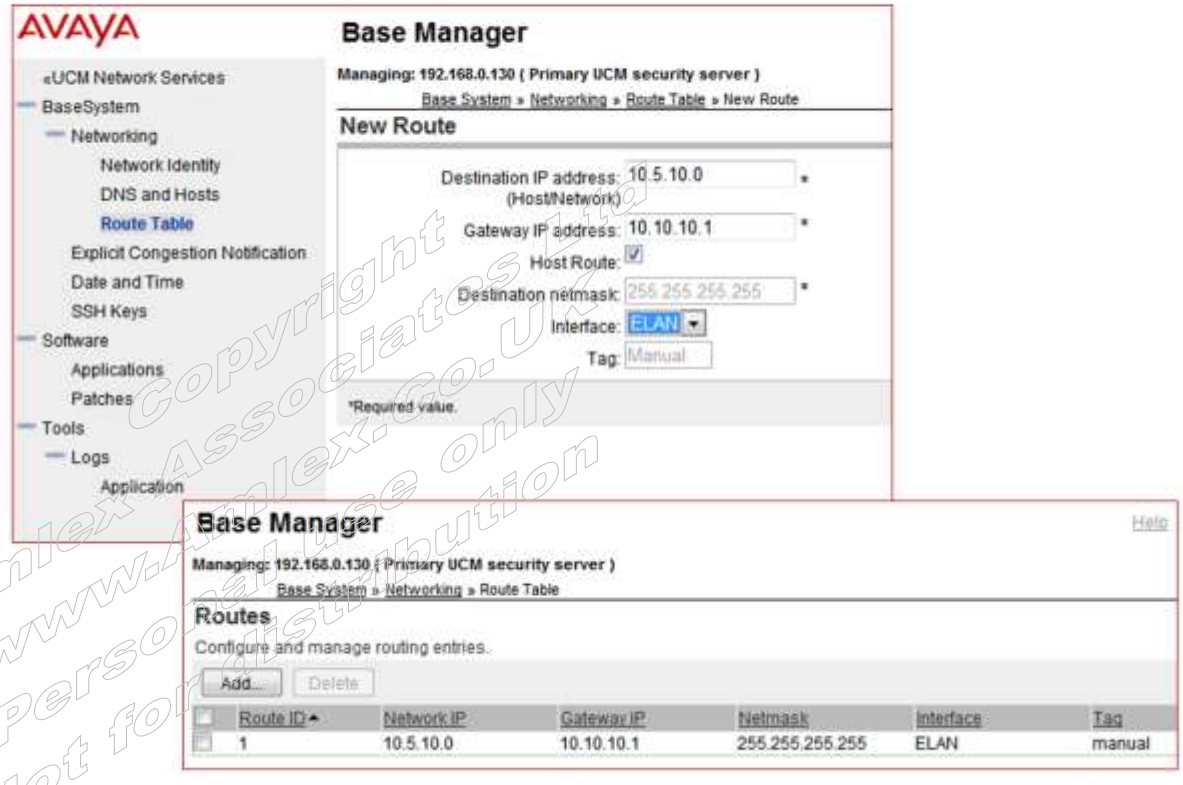
_____

Add Route to CoRes Server

Because the CoRes server has all its IP networking details carried out by the Linux server it resides on not IP configuration is possible from LD 117. This however can lead to issues where a system has media gateways distributed on different sites with different ELAN addresses.

This is caused by the Linux server which during configuration sets the TLAN network as its default gateway for any unknown addresses. Thus when an unknown ELAN address is encountered it is sent out via the TLAN rather than the ELAN network. If the TLAN is not fully routed to the ELAN networks connections will not be made or can be rejected as they appear from the wrong interface.

To overcome this a route must be added into the Linux server pointing specifically to the ELAN as shown here. In this way all



Amlex Associates Ltd
www.Amlex.co.UK
Copyright
Personal use only
Not for distribution

397

Notes

_____

_____

_____

_____

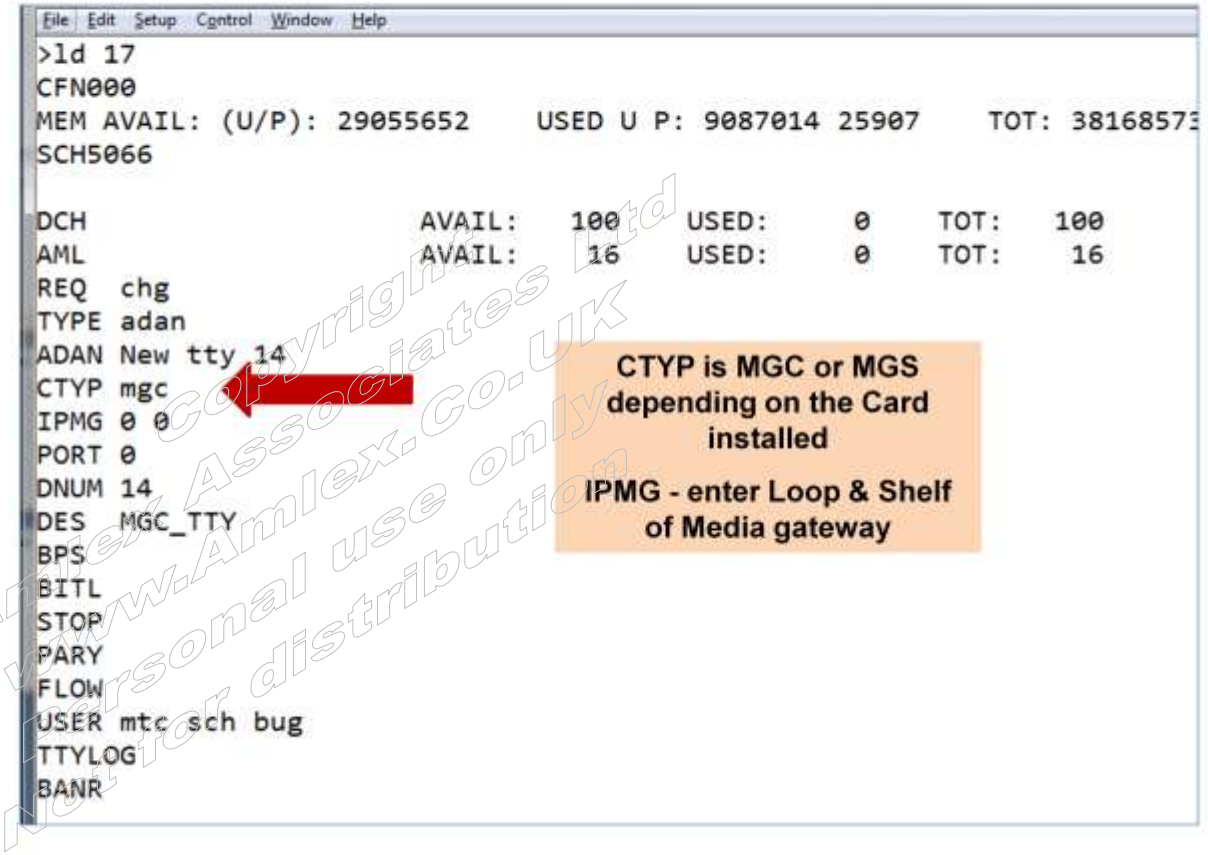
Copyright Amlex Associates Ltd

MGC/MGS TTY Port Configuration

To configure the serial ports on the MGC card for use as TTY's follow the steps as shown.

There are three ports on the MGC 0,1 and 2 which can be used.

Note on a CoRes server this will give a direct connection to the Overlays without the use of **cslogin** or **csconsole.**



Copyright Amlex Associates Ltd
www.Amlex.co.uk
Personal use only
Not for distribution

Notes

_____

_____

_____

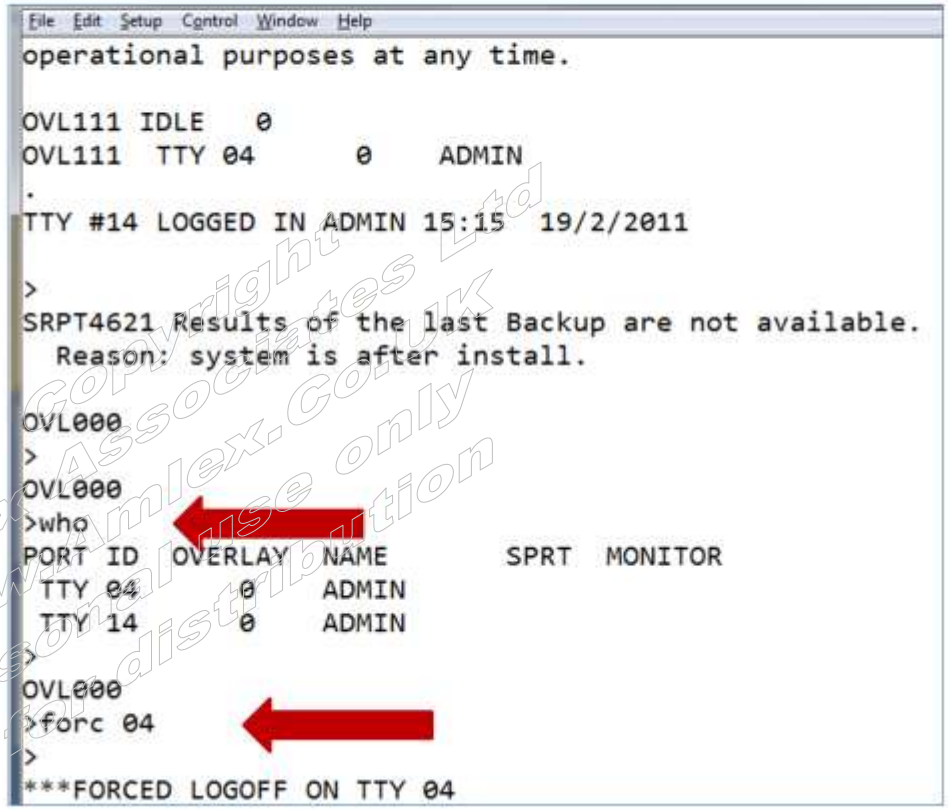
_____

Force Out Logged in TTY

Occasionally a terminal will be left logged in on a switch and also in one of the overlays preventing access by other users.

To log the terminal out remotely first find their TTY number using the command WHO in LD 0. To log that TTY out enter the command FORC <TTY no.>.

You must have ADMIN2 or Network Administrator rights to do this.



399

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd

Set the Time in Linux

Getting the correct time setup across all devices in the system can be difficult with the CS1K so the following can help

LD 2 TTAD & STAD to print and set time for SA and HA (VxWorks Call Servers)

To set the NTP for a VxWorks call server:-

In LD 117 –

ENL/DIS NTP
Enable or Disable NTP

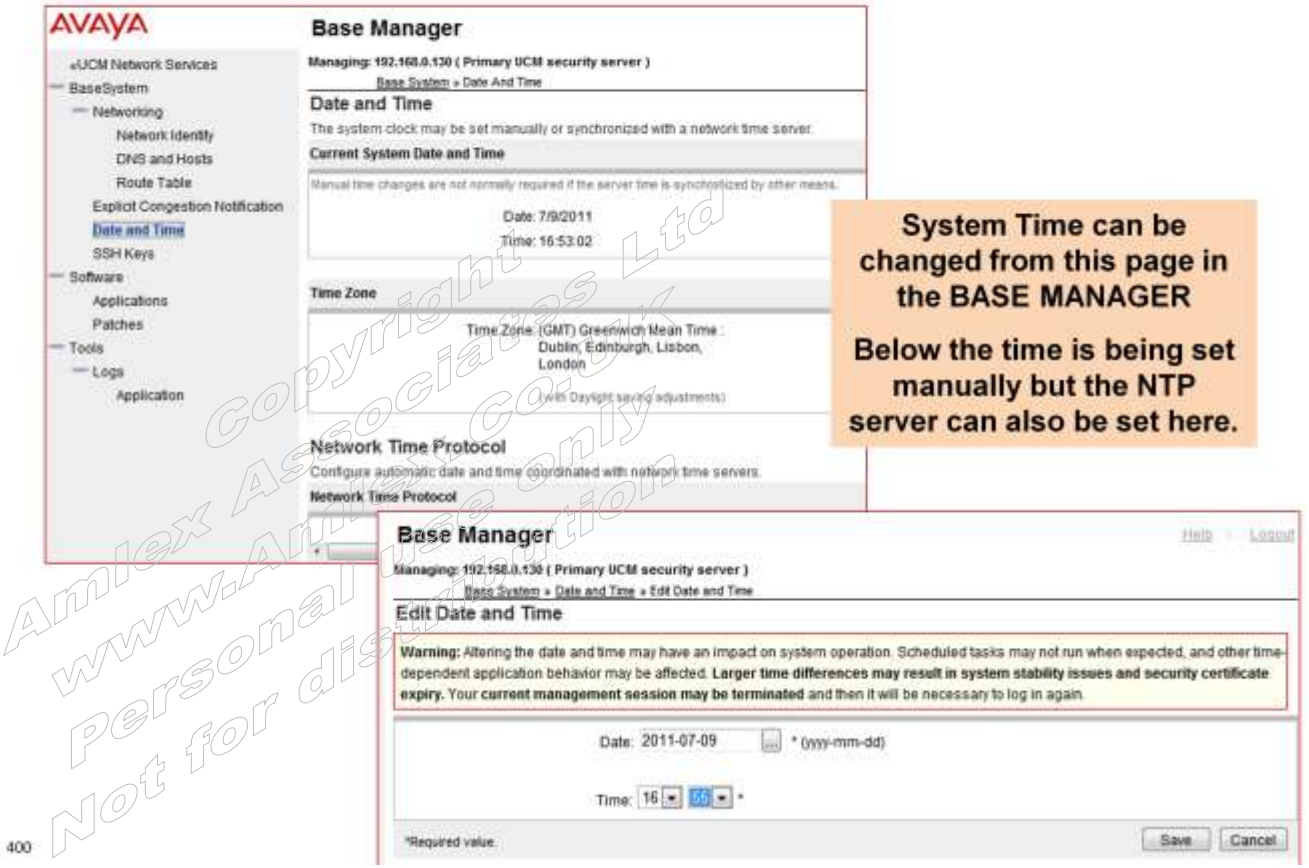
CHG NTP IPADDR 10.10.10.202
Change IP Address of NTP Server

STAT NTP
Check setup of NTP for Call Server

SYNC NTP MANUAL or BACKGROUND
Execute NTP Sync now or overnight

You may also need to adjust the UTC offset for the call server.

CHG UTCOFFSET <+/-hh:mm>
Changes UTC offset by specified amount


AVAYA
Base Manager
«UCM Network Services
BaseSystem
Networking
Network Identity
DNS and Hosts
Route Table
Explicit Congestion Notification
Date and Time
SSH Keys
Software
Applications
Patches
Tools
Logs
Application
Managing: 192.168.0.130 (Primary UCM security server)
Base System » Date And Time
Date and Time
The system clock may be set manually or synchronized with a network time server.
Current System Date and Time
Manual time changes are not normally required if the server time is synchronized by other means.
Date: 7/9/2011
Time: 16:53:02
Time Zone
Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
(with Daylight saving adjustments)
Network Time Protocol
Configure automatic date and time coordination with network time servers.
Network Time Protocol
System Time can be changed from this page in the BASE MANAGER
Below the time is being set manually but the NTP server can also be set here.
Base Manager
Help | Logout
Managing: 192.168.0.130 (Primary UCM security server)
Base System » Date and Time » Edit Date and Time
Edit Date and Time
Warning: Altering the date and time may have an impact on system operation. Scheduled tasks may not run when expected, and other time-dependent application behavior may be affected. Larger time differences may result in system stability issues and security certificate expiry. Your current management session may be terminated and then it will be necessary to log in again.
Date: 2011-07-09
* (yyyy-mm-dd)
Time: 16 55 *
*Required value.
Save
Cancel
400

Amlex Associates Ltd Copyright www.Amlex.co.uk Personal use only Not for distribution

Notes

_____

_____

_____

_____

Copyright Amlex Associates Ltd